AirGuard™ Wireless Access Point
User's Guide

Model 3e-525C–2

3e Technologies International
700 King Farm Blvd., Suite 600
Rockville, MD 20850
(301) 670-6779 www.3eti.com

29000155-001 A

publ. 05/02/05

This page intentionally left blank.

3e Technologies International's AirGuard™ Wireless Access Point User's Guide

Model 3e-525C–2

Copyright © 2005 3e Technologies International. All rights reserved. No part of this documentation may be reproduced in any form or by any means or to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3e Technologies International.

3e Technologies International reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3e Technologies International to provide notification of such revision or change.

3e Technologies International provides this documentation without warranty, term or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms, or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3e Technologies International may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time. Certain features listed may have restricted availability and/or are subject to change without notice - please confirm material features when placing orders.

If there is any software or removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the printed documentation, or on the removable media in a readable file such as license.txt or the like. If you are unable to locate a copy of the license, contact 3e Technologies International and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States Government agency, then this documentation and the product described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as “Commercial Computer Software” as defined in DFARS 252.227-7014 (June 1995) or as a “commercial item” as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3e Technologies International’s standard commercial license for the software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

3e Technologies International and the 3e Technologies International logo are registered trademarks.

Windows is a registered trademark of Microsoft Corporation. Any other company and product name mentioned herein is a trademark of the respective company with which they are associated.

EXPORT RESTRICTIONS

This product contains components, software, and/or firmware exported from the United States in accordance with U. S. export administration regulations. Diversion contrary to U.S. law is prohibited.

Table of Contents

Chapter 1: Introduction 1
- Basic Features 2
- Wireless Basics 2
  - 802.11b 3
  - 802.11a 3
  - 802.11b/g Mixed 3
  - 802.11 Super G and Turbo A 3
  - Network Configuration 4
  - Access Point Configurations 4
    - Possible AP Topologies 4
  - Bridging 5
  - Data Encryption and Security 6
  - SSID 6
  - WEP 6
  - WPA with TKIP/ AES-CCMP 6
  - AES 7
  - MAC Address Filtering 7
  - DHCP Server 7
  - Operator Authentication and Management 7
- Management 8
- 3e–525C–2 Navigation Options 9

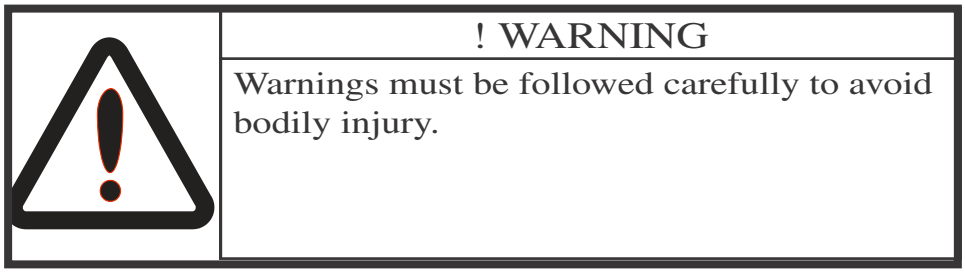
Chapter 2: Hardware installation 11
- Preparation for Use 11
- Installation Instructions 12
- Minimum System and Component Requirements 12
- Connectors and Cabling 13
- Bridge Transmit Distance 14
- Bridge Antenna Location 14
- Outdoor Protection Kit Installation 15
  - Earth Ground Connection 16
  - Lighnting Arrestor Installation 16
- Antenna Installation 17
  - Sealing Antenna Connections 17
- Mounting Kit Setup 18
  - The Indicator Lights 18

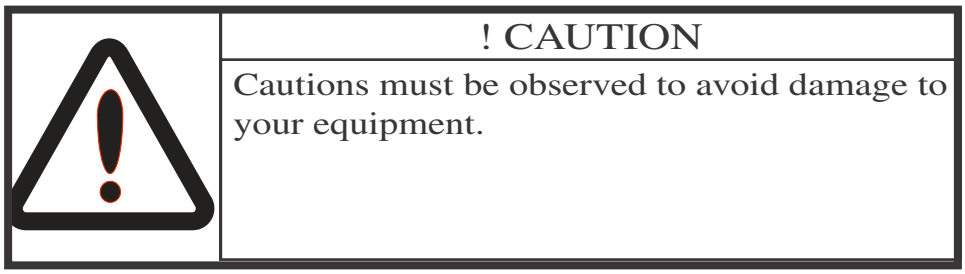
Chapter 3: Access Point Configuration 21
- Introduction 21
- Preliminary Configuration Steps 21
- Initial Setup using the “Local” Port 22
- System Configuration 24
  - General 24
  - WAN 25
  - LAN 26
- Wireless Access Point Configuration 27
  - General 27
  - Security 30
    - No Encryption 30
    - Static WEP Encryption 31
    - 802.11i and WPA 32
  - MAC Address Filtering 34
  - Rogue AP Detection 35

Advanced....36
Wireless Bridge....36
Services Settings....37
DHCP Server....37
SNMP Agent....38
User Management....39
List All Users....39
Add New User....40
Monitoring/Reports....41
System Status....41
Bridging Status....42
Bridge Site Map....43
Wireless Clients....44
Adjacent AP List....44
DHCP Client List....45
System Log....45
Web Access Log....46
Network Activity....46
System Administration....47
System Upgrade....47
Firmware Upgrade....47
Local Configuration Upgrade....48
Factory Default....49
Remote Logging....49
Reboot....50
Utilities....50
Chapter 4: Wireless Bridge Configuration....51
Introduction....51
Wireless Bridge — General....52
Auto-forming Wireless Bridging....52
Manual Bridging....55
Monitoring....58
Wireless Bridge — Encryption....58
Setting Up Bridging Type....59
Point-to-Point Bridge Configuration....59
Point-to-Point Bridging Setup Guide - Manual Mode....60
Point-to-Point Bridging Setup Guide - Auto Mode....60
Point-to-Multipoint Bridge Configuration....64
Point-to-Multipoint Bridging Setup Guide - Manual Mode....65
Point-to-Multipoint Bridging Setup Guide - Auto Mode....65
Repeater Bridge Configuration....66
Repeater Bridging Setup Guide - Manual Mode....66
Repeater Bridging Setup Guide - Auto Mode....67
Chapter 5: Technical Support....69
Manufacturer's Statement....69
Radio Frequency Interference Requirements....69
Glossary....G-a

SAFETY INFORMATION

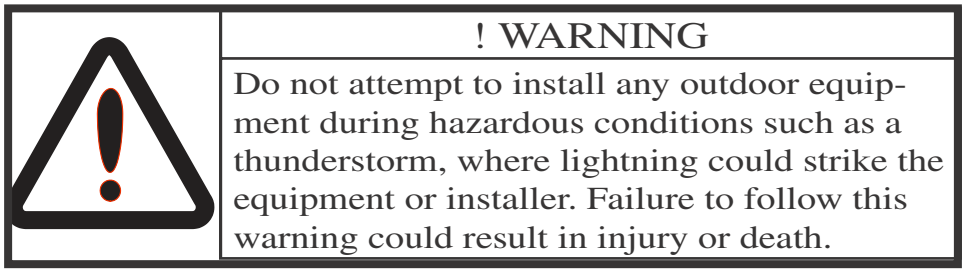
Please follow thes guidelines when installing and using the 3e–525C–2 product.





NOTE: Notes contain important information about this product.

The following warnings appear in this manual.


! WARNING
Do not attempt to install any outdoor equipment during hazardous conditions such as a thunderstorm, where lightning could strike the equipment or installer. Failure to follow this warning could result in injury or death.

This page intentionally left blank.

Chapter 1: Introduction

This manual covers the installation and operation of the 3e Technologies International's 3e–525C–2 Wireless Access Point. The 3e–525C–2 is a ruggedized access point/bridge which is intended for use in industrial and external environments. It accommodates 802.11a/b/g, 802.11g Super, and 802.11a Turbo WLAN access and uses Power over Ethernet (PoE) access to the Ethernet WAN to eliminate the need for internal access point power supply units (AC-DC converters) and 110-220V cabling installations. The wireless LANs can include mobile devices such as handheld Personal Data Assistants (PDAs), mobile web pads, and wireless laptops.

If encryption is desired for the WLAN, you can select None, Static WEP, or WPA. WPA uses TKIP or AES-CCMP so you can employ legacy client WEP cards and still secure the wireless band.

The 3e–525C–2 incorporates Power over Ethernet. The PoE interface on the 3e–525C–2 is compatible with commercial vendor "injected power" hub units.

The 3e–525C–2 includes AES cryptographic modules for wireless encryption and HTTPS/TLS, for secure web communication. In addition, it contains the capability to use the traditional WEP algorithm, either as static WEP or managed under WPA. The 3e–525C–2 has an Ethernet WAN interface for communication to the wired LAN backbone, Ethernet LAN local port for purposes of initial setup and configuration, and two wireless AP antennas for communicating on the 802.11a/b/g frequencies. Further, it has the capability for use of an external (remote) antenna, for bridging, using the 802.11b/g Mixed, 802.11a, 802.11g Super, 802.11a Turbo frequencies.

Basic Features

The 3e–525C–2 is housed in a sturdy case which is not meant to be opened except by an authorized technician for maintenance or repair. If you wish to reset to factory settings, use the reset function available through the GUI-based management module or press and hold the reset button on the front of the unit for 10 seconds.

The 3e–525C–2 is wall-mountable.

It has the following features:

- Ethernet uplink WAN port
- Local Ethernet LAN port (for configuration only)
- Wireless AP with operating range of 2000+ feet
- Wireless Bridge
- Power over Ethernet (PoE)
- Above average temperature range for extreme environments (with TEC option)
- HTTPS/TLS secure Web
- DHCP client
- Bandwidth control
- Adjustable Radio Power
- MAC address filtering
- Load Balancing
- Rogue AP Detection

The following security modules have been implemented in the 3e–525C–2 .

- AES (128 bit) for Bridge
- WEP (64, 128, and 152 bit) for AP
- WPA (pre-share key and TKIP/AES-CCMP) for AP
- 802.11i/WPA2 (128 bit) for AP

Wireless Basics

Wireless networking uses electromagnetic radio frequency waves to transmit and receive data. Communication occurs by establishing radio links between the wireless access point and devices configured to be part of the WLAN.

For wireless devices to communicate with the 3e–525C–2 , they must meet the following conditions:

- The wireless device and wireless access point must have been configured to recognize each other using the SSID (a unique ID assigned in setup so that the wireless device is seen to be part of the network by the 3e–525C–2);
- Encryption and authentication capabilities and types enabled must conform; and
- If MAC filtering is used, the 3e–525C–2 must be configured to allow the wireless device's MAC address to associate (communicate) with the 3e–525C–2 wireless interface.

802.11b

The IEEE 802.11b standard ratified by IEEE, establishes a stable standard for compatibility. A user with an 802.11b product can use any brand of access point with any other brand of client hardware that is built to the 802.11b standard for basic interconnection. 802.11b devices provide 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps depending on signal strength) in the 2.4 GHz band.

802.11g

Because 802.11g is backwards-compatible with 802.11b, it is a popular component in LAN construction. 802.11g broadens 802.11b's data rates to 54 Mbps within the 2.4 GHz band using OFDM (orthogonal frequency division multiplexing) technology.

802.11a

The IEEE 802.11a standard is an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS.

802.11b/g Mixed

802.11b/g combines 802.11b and 802.11g data rates to offer a broader range. In this mode, all transmissions will be at the highest data rate available.

802.11 Super G and Turbo A

802.11 Super G and 802.11 Turbo A technologies provide speed and throughput of more than double standard wireless LAN technologies in networking products such as PCs, access points, routers and PC cards. It is very helpful to users who require additional bandwidth (over standard WLAN technologies) that results in higher throughput necessary for a variety of functions such as: streaming media (video, DVD, MPEG), VoIP, etc., or for providing multiple users on a single WLAN with optimal speeds despite network demand.

108 Mbps is the *maximum link speed* available and the typical MAXIMUM end-user throughput ranges from approximately 40 Mbps to 60+ Mbps, depending on application demand and network environment.

NOTE: Super G's channel bonding feature can significantly degrade the performance of neighboring 2.4GHz WLANs that don't use Super G, because there isn't enough room in the 2.4GHz wireless LAN spectrum for the increased spectrum used by channel bonding. Moreover, Super G doesn't check to see if 11b or 11g standards-compliant devices are in range before using its non-standard techniques.

Network Configuration

The 3e–525C–2 is an access point with bridging setup capability:

- Access point/Gateway plus:
- Wireless bridging with choice of:
  - Point-to-point setup
  - Point-to-multipoint setup
  - Repeater setup

Bridging actually has more choices, but the above choices are popular and are discussed later in this user guide (Chapter 4).

Access Point Configurations

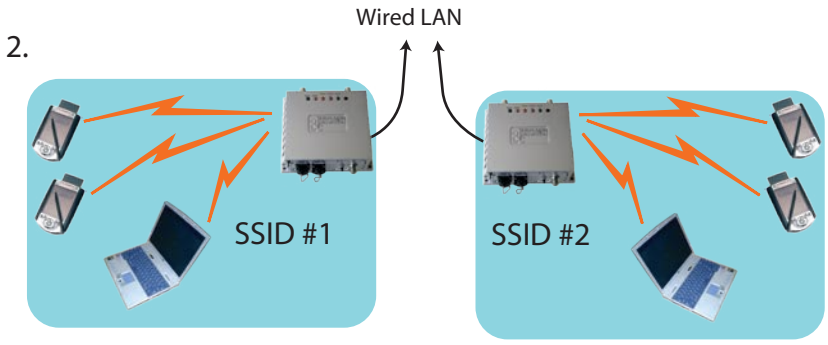
When a 3e–525C–2 is used as an access point, IP addresses for wireless devices are typically assigned by the wired network's DHCP server. The wired LAN's DHCP server assigns addresses dynamically, and the AP virtually connects wireless users to the host wired network. All wireless devices connected to the AP are configured on the same subnetwork as the wired network interface and can be accessed by devices on the wired network.

Possible AP Topologies

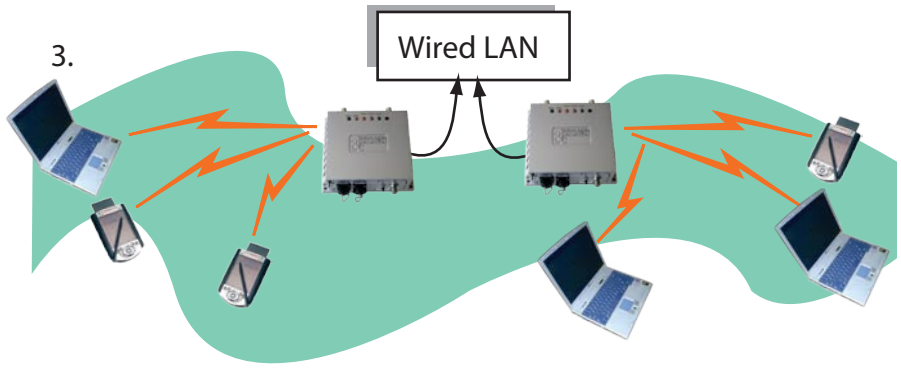
1. An access point can be used as a stand-alone AP without any connection to a wired network. In this configuration, it simply provides a stand-alone wireless network for a group of wireless devices.

1.

2. There can be multiple APs connected to an existing Ethernet network to bridge between the wired and wireless environments. Each AP can operate independently of the other APs on the LAN. Multiple APs can coexist as separate individual networks at the same site with a different network ID (SSID).



3. The last and most prevalent use is multiple APs connected to a wired network and operating off that network's DHCP server to provide a wider coverage area for wireless devices, enabling the devices to "roam" freely about the entire site. The APs have to use the same SSID. This is the topology of choice today.



Bridging

The wireless bridging function in the 3e–525C–2 allows use as a bridge, in a number of alternate configurations, including the following popular configurations:

- Point-to-point bridging of 2 Ethernet Links;
- Point-to-multipoint bridging of several Ethernet links;
- Repeater mode (wireless client to wireless bridge.)

Data Encryption and Security

The 3e–525C–2 Wireless Access Point includes advanced wireless security features. Over the AP band, you have a choice of no security, Static WEP, or WPA. Some level of security is suggested. Static WEP gives you a choice of 64-bit, 128-bit, or 152-bit encryption. WPA includes the option of using a WPA pre-shared key or, for the enterprise that has a Radius Server installed, configuration to use the Radius Server for key management with either TKIP or AES-CCMP. Bridging encryption is established between 3e–525C–2's and includes use of AES-ECB 128-bit encryption (approved by the National Institute of Standards and Technology (NIST) for U.S. Government and DoD agencies).

SSID

The Service Set ID (SSID) is a string used to define a common roaming domain among multiple wireless access points. Different SSIDs on access points can enable overlapping wireless networks. The SSID can act as a basic password without which the client cannot connect to the network. However, this is easily overridden by allowing the wireless AP to broadcast the SSID, which means any client can associate with the AP. SSID broadcasting can be disabled in the 3e–525C–2 setup menus.

WEP

WEP is an older encryption standard but is preferable to no encryption. If the 3e–525C–2 is configured with WEP encryption, it is compatible with any 802.11b PC Card configured for WEP.

WPA with TKIP/ AES-CCMP

WPA, an interim standard developed by the WiFi Alliance, combines several technologies. It includes the use of the 802.1x standard and the Extensible Authentication Protocol (EAP). In addition, it uses, for encryption, the Temporal Key Integrity Protocol (TKIP) and WEP 128-bit encryption keys. Finally, a message integrity check (MIC) is used to prevent an attacker from capturing and altering or forging data packets. In addition, it can employ a form of AES called AES-CCMP.

WPA is a subset of the 802.11i standard and is expected to maintain forward compatibility.

AES

The Advanced Encryption Standard (AES) was selected by National Institute of Standards and Technology (NIST) in October 2000 as an upgrade from the previous DES standard. AES uses a 128-bit block cipher algorithm and encryption technique for protecting computerized information.

The 3e–525C–2 uses AES for the bridging channel.

MAC Address Filtering

The MAC address, short for *Media Access Control address,* is a hardware address that uniquely identifies each node of a network. In IEEE 802 networks, the Data Link Control (DLC) layer of the OSI Reference Model is divided into two sub-layers: the *Logical Link Control (LLC) layer* and the *Media Access Control (MAC) layer.* The MAC layer interfaces directly with the network media. Consequently, each type of network media requires a unique MAC address.

Authentication is the process of proving a client identity. The 3e–525C–2 access points, if set up to use MAC address filtering, detect an attempt to connect by a client and compare the client's MAC address to those on a predefined MAC address filter list. Only client addresses found on the list are allowed to associate. MAC addresses are pre-assigned by the manufacturer for each wireless card.

DHCP Server

The DHCP function is accessible only from the local LAN port to be used for initial configuration.

Operator Authentication and Management

Authentication mechanisms are used to authenticate an operator accessing the device and to verify that the operator is authorized to assume the requested role and perform services within that role.

Access to the management screens for the 3e–525C–2 requires knowledge of the assigned operator ID and Password. The Factory defaults are:

- ID: crypto
- Password: officer

The Crypto Officer initially installs and configures the 3e–525C–2 after which the password should be changed from the default password. The ID and Password are case sensitive.

Management

After initial setup, maintenance of the system and programming of security functions are performed by personnel trained in the procedure using the embedded gui-based management screens.

The next chapter covers the basic procedure for setting up the hardware.

3e–525C–2 Navigation Options
System Configuration
General
WAN
LAN
Wireless Access Point
General
Security • None • Static WEP • 802.11i and WPA
MAC Address Filtering
Rogue AP Detection
Advanced
Wireless Bridge
General • Monitoring
Encryption • AES (128-bit)
MAC Address Filtering
Services Settings
DHCP Server
SNMP Agent
User Management
List All Users • Edit/Delete
Add New User
Monitoring Reports
System Status
Bridging Status
Bridging Site Map
Wireless Clients
Adjacent AP List
DHCP Client List
System Log
Web Access Log
Network Activities
System Administration
System Upgrade • Firmware Upgrade • Local Configuration Upgrade
Factory Default
Remot Logging
Reboot
Utilities

This page intentionally left blank.

Chapter 2: Hardware installation

Preparation for Use

The 3e Technologies International's 3e–525C–2 Wireless Access Point requires physical mounting and installation on the site, following a prescribed placement design to ensure optimum operation and roaming.

FCC Regulations require that the 3e–525C–2 be professionally installed by an installer certified by the National Association of Radio and Telecommunications Engineers or equivalent institution.

The 3e–525C–2 operates with Power over Ethernet (PoE) which requires the installation of a separate Power injector which “injects” DC current into the Cat5 cable. There are two versions of the 3e–525C–2 available, the standard version with a temperature range of -5 degrees C to +50 degrees C, and there is the extended temperature range product with a range of -30 degrees C to +70 degrees C. The latter version of the product employs ThermoElectric Cooler (TEC) technology to extend the product into the higher temperature environment.

The TEC Technology comes with a price, it requires power to transfer the heat. Unfortunately, this raises the electric current requirement to 25 watts, beyond the 802.3af specification of 15.4 watts. To ensure that the 3e–525C–2 with TEC option is provided with the power it requires, an extended range PoE power injector is required such as the 3eTI Model 3e-POE-1 or Hyperlink Technologies Model BT-CAT5-P1.

The 3e–525C–2 package includes the following items:

- The 3e–525C–2 Wireless Access Point
- 2 attachable 5dBi omni-directional antennas
- 2 meter LAN Ethernet cable (RJ-45 to RJ-45)
- Documentation as PDF files (on CD-ROM)
- Registration and Warranty cards

The following items are options:

- Power Injector, POE, 50W (model 3e-POE-1, p/n 90000831-001)
- Power Cord, POE Injector, European version (p/n 90000832-001)
- Power Cord, POE Injector, UK version (p/n 90000833-001)
- 3 meter antenna extension cable
- Outdoor Protection Kit

The bridge antenna port is used when configuring the unit to be used as a bridge. The port uses an omni-directional antenna.

The 3e–525C–2 can be mounted outdoors on a high post to achieve the best bridge result. If mounted outdoors, the outdoor protection kit must be used to prevent lightning damage.

To comply with FCC RF exposure compliance requirements, the antennas used with the 3e–525C–2 must be installed with a minimum separation distance of 20 cm from all persons, and must not be co-located or operated in conjunction with any other antenna or transmitter. Installation should be accomplished using the authorized cables and/or connectors provided with the device or available from the manufacturer/distributor for use with this device. Changes or modifications not expressly approved by the manufacturer or party responsible for this FCC compliance could void the user's authority to operate the equipment.

Installation Instructions

The 3e–525C–2 is intended to be installed as part of a complete wireless design solution.

This manual deals only with the 3e–525C–2 device. The purpose of this chapter is the description of the device and its identifiable parts so that the user is sufficiently familiar to interact with the physical unit. Preliminary setup information provided below is intended for information and instruction of the wireless LAN system administration personnel.

It is intended that the user not open the unit. Any maintenance required is limited to the external enclosure surface, cable connections, and to the management software (as described in chapter three through five) only. A failed unit should be returned to the manufacturer for maintenance.

Minimum System and Component Requirements

The 3e–525C–2 is designed to be attached to the wall at appropriate locations. To complete the configuration, you should have at least the following components:

- PCs with one of the following operating systems installed: Windows NT 4.0, Windows 2000 or Windows XP;
- A Wi-Fi compatible 802.11a/b/g device for each computer that you wish to wirelessly connect to your wireless network. (For wireless cards, 3eTI recommends that you select the 3e-110 PC Card with 3e-010F Crypto Client software (sold separately) or install the 3e-010F software with any compatible PC Card. (If you will be using WEP, the 3e-010F software is not required);
- Access to at least one laptop or PC with an Ethernet card and cable that can be used to complete the initial configuration of the unit.
- A Web browser program (such as Microsoft Internet Explorer 5.5

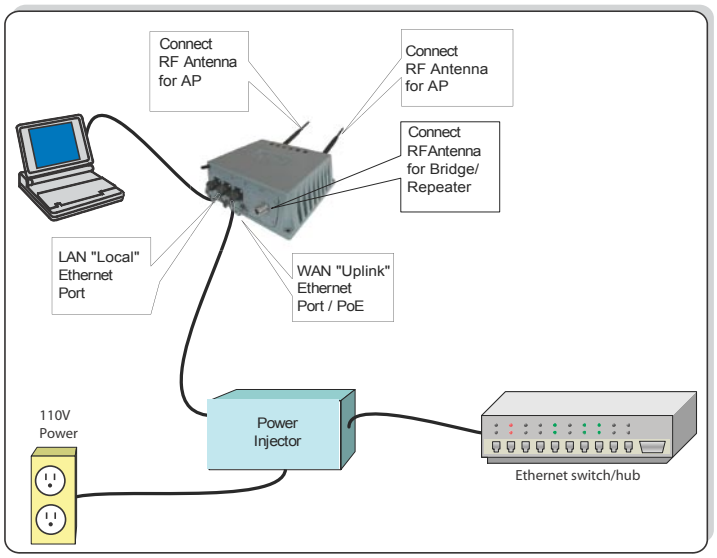
or later, or Netscape 6.2 or later) installed on the PC or laptop you will be using to configure the Access Point.

- TCP/IP Protocol (usually comes installed on any Windows PC.)

Connectors and Cabling

The following illustration shows the external connectors on the 3e–525C–2.

The WAN connector is used to connect the 3e–525C–2 to the organization's LAN. The WAN connector is routed from the unit to the power injector which runs DC power through the Ethernet cable to the unit. The Ethernet cable is thus run from the 3e–525C–2 to the power injector which is then connected to a power source and the wired LAN. A second (LAN Port) Ethernet connector is designed for use during initial configuration only. This uses an RJ45 cable to connect the 3e–525C–2 to a laptop. The following diagram demonstrates the setup.



Bridge Transmit Distance

Normally, the bridge need transmit RF signal to another bridge device at long distance. You may need to calculate the RF link Budget as reference. The equation of RF link budget is:

Fade Margin = received signal – receiver threshold

Where

Received signal = Transmitter power – Transmitter cable loss + Transmitter antenna gain – free space path loss + Receiver antenna gain – Receiver cable loss

Received threshold = Received sensitivity

Free Space Path Loss

Using below Free Space Loss Formula to calculate free space path loss

$$L_p = 96.6 + 20\log_{10} F + 20\log_{10} D$$

Where

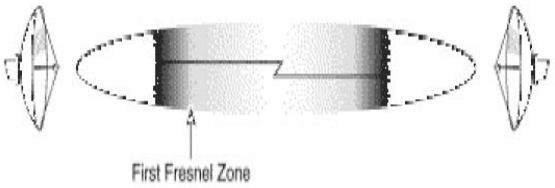
L_p = free space path loss between antennas

F = frequency in GHz

D = path length in miles

Bridge Antenna Location

When as bridge device, the 3e-525C may need to be mounted outdoors on a high place to achieve the best bridge result. The Fresnel zone and Earth bulge dominate to decide how high that the unit's Antenna need be put. The total antenna height equals the width of Fresnel zone plus the height of earth bulge.



The Fresnel zone is the area around the visual line-of-sight that radio waves spread out into after they leave the antenna. This area must be clear or else signal strength will weaken. The rule of thumb is that 60% of the Fresnel zone must be clear of obstacles. Typically, 20% Fresnel Zone blockage introduces little signal loss to the link. Beyond 40% blockage, signal loss will become significant.

The equation of the width of Fresnel Zone is:

$$W = 43.3 \times \sqrt{\frac{D}{4F}}$$

Where

W = Width of the Fresnel Zone (in feet)

D = Distance between the antennas (in miles)

F = Frequency in GHz

When the transmit distance of RF signal is longer than seven miles, the curvature of the earth may be a factor and require the antenna put at higher location. The additional antenna height can be calculated by below formula:

$$H = \frac{D^2}{8}$$

Where

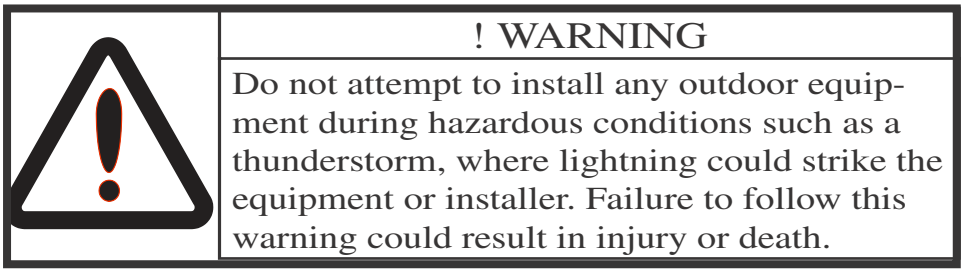
H = Height of earth bulge (in feet)

D = Distance between antennas (in miles)

Outdoor Protection Kit Installation

If any portion of this assembly, either the 3e–525C–2 unit or any attached antenna, is to be used outside, the proper Outdoor Protection Kit ***must*** be installed. This kit contains lightning arrestors for each antenna and the required cabling to connect these items to the common grounding stud on the 3e–525C–2 unit.

NOTE: You (the user) are required to ensure that the connection to a proper earth ground is made by properly certified and authorized personnel and must conform to all applicable codes and regulations. The materials required to connect to a proper ground are defined by local conditions and must be procured locally to ensure the correct safety environment is achieved. The cable used to connect to a proper ground must be AWG 10 or heavier. This cable should be kept as short as possible.


! WARNING
Do not attempt to install any outdoor equipment during hazardous conditions such as a thunderstorm, where lightning could strike the equipment or installer. Failure to follow this warning could result in injury or death.

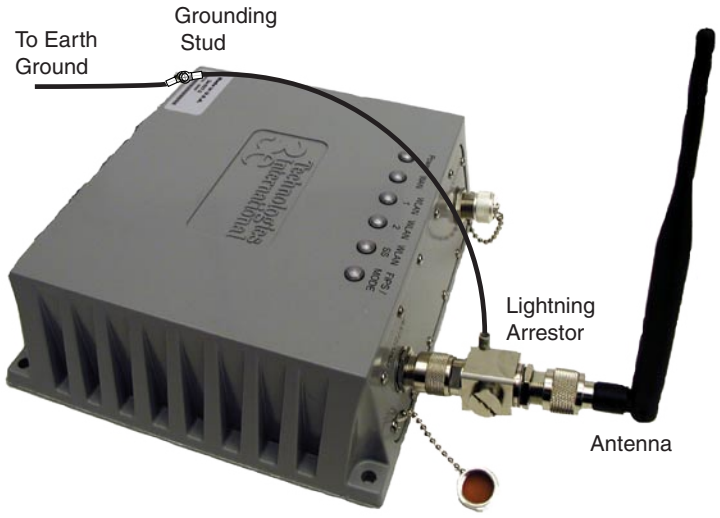
Earth Ground Connection

Attach the earth ground ring terminal to the 3e–525C–2's grounding stud. Make sure the ring terminal is against the unit's metal case. The earth ground ring terminal should be the first connection on the unit's grounding stud.

NOTE: The cable used to connect to a proper earth ground must be AWG 10 or heavier. This cable should be kept as short as possible

Lighnting Arrestor Installation

To install the lightning arrestor, attach one end of the lightning arrestor to the 3e–525C–2's antenna connector. Attach the antenna (or the antenna cable) to the other end of the lightning arrestor.



Attach the ring terminal from the Lightning Arrestors' ground cable to the grounding stud on the 3e–525C–2 unit. The lightning arrestor's ring terminal should be attached to the unit after the earth ground ring terminal is attached.

Perform this same procedure for every antenna installed on the unit.

It is recommended that this Outdoor Protection Kit be replaced every three years. If the unit is operated in an area subject to intense lightning activity, it is recommended that the Outdoor Protection Kit be replaced every year.

Antenna Installation

The 3e–525C–2 ships with two 5dBi omni-directional antennas. These antennas should be connected to the AP antenna connectors located on the rear of the unit.

NOTE: Make sure a lightning arrestor is installed between the unit and the antenna. See the previous section.

If you are not using the access point function then you do not need the AP antennas. Make sure during your configuration set up that you go to the **Wireless Access Point—General** screen and set the Tx Pwr Mode to Off (see Chapter 3).

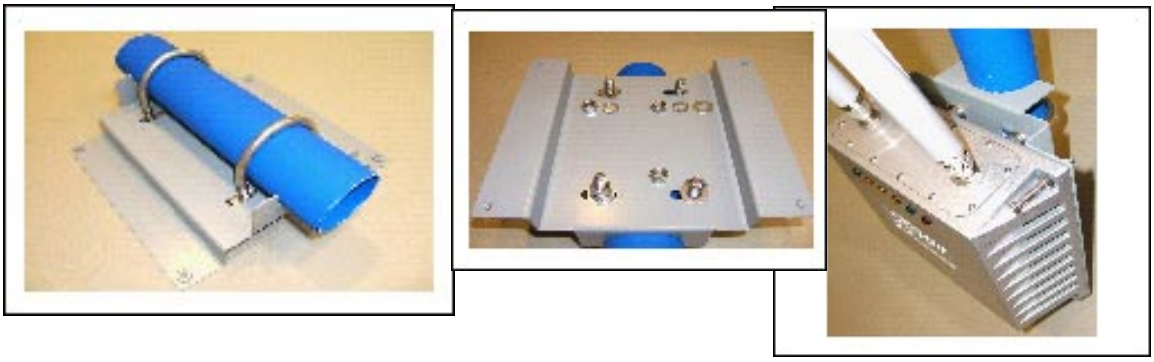
Sealing Antenna Connections

Once all antennas have been installed, the connections should be sealed to protect them from the exterior harsh environment. Use a self amalgamating polyisobutylene tape which, over a period of hours, adheres to itself and forms a single amalgamated rubber molding conforming to the shape of the item it is covering. Once the tape is in place for several hours, it forms a shaped rubber molding that is resistant to water and most solvents. It remains stable over a wide temperature range and degrades very slowly in sunlight. If you need to remove the tape after it has sealed for 30 minutes or more, cut it away with a sharp knife.

The bridge antenna port is located on the front of the 3e–525C–2. To obtain the best performance, the bridge antenna should be placed away from the AP antennas. Use a 1.5 meter low loss antenna cable to connect a directional antenna to the 3e–525C–2. The maximum gain for the directional antenna should be 14 dBi.

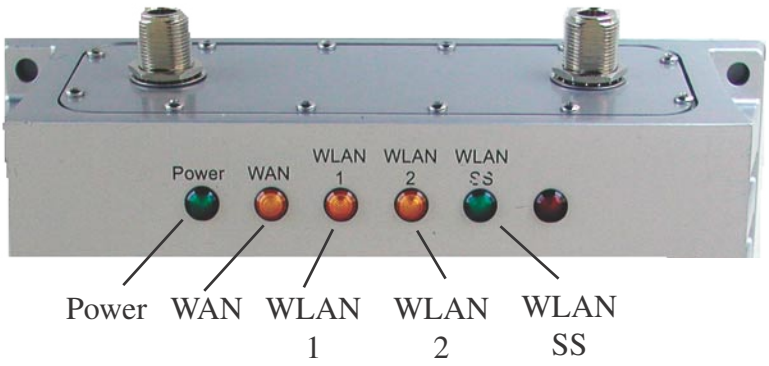
Mounting Kit Setup

To mount the 3e–525C–2 outdoors, you should choose a suitable post to mount the unit high in the air. Use the U-ring, screws and nuts to attach the mounting plate to the post. Next attach the 3e–525C–2 to the mounting plate with screws.



The Indicator Lights

The top panel of the 3e–525C–2 contains a set of indicator lights (Light Emitting Diodes or LEDs) that help describe the state of various networking and connection operations.



LED	Description
Power	The Power indicator LED informs you when the gateway is on or off. If this light is on, the gateway is on; if it is not on, the gateway is off.
WAN	This light indicates the state of your connection to the organization's Ethernet LAN network. When on, the WAN light indicates that the unit is connected to the network. When the WAN light is off, the gateway does not have an active connection to the network.
WLAN1 Activity	This light may be steady or blinking and indicates that information is passing through the AP connection.
WLAN2 Activity	This light may be steady or blinking and indicates that information is passing through the Bridge connection.
WLAN Signal Strength	The Strength LED indicator indicates the strength of the Bridge connection (WLAN2). 1. LED Off: means no connection on the bridge side, or the signal is very weak 2. LED blinks slowly (every 1 second): means there is a connection, and the signal quality is poor 3. LED blinks fast: means there is a connection, and the signal quality is good 4. LED steady on: means there is a connection, and the signal quality is excellent

This page intentionally left blank.

Chapter 3: Access Point Configuration

Introduction

The 3e–525C–2 comes with the capability to be configured as an access point. As it incorporates two separate 802.11 wireless cards, one for configuring a local WLAN and one for use in bridging, it can also be configured for bridging, with the access point configuration on the WLAN side. Configuration for bridging is discussed in Chapter 4.

Preliminary Configuration Steps

For preliminary installation the 3e–525C–2 network administrator may need the following information:

- PC/laptop with one of the following operating systems installed: Windows NT 4.0, Windows 2000, or Windows XP
- A web browser program, such as Microsoft Internet Explorer 5.5 or later, or Netscape 6.2 or later, installed on the PC/laptop used for configuring the access point
- IP address – a list of IP addresses available on the organization's LAN that are available to be used for assignment to the AP(s)
- Subnet Mask for the LAN
- Default IP address of the 3e–525C–2
- DNS IP address
- SSID – an ID number/letter string that you want to use in the configuration process to identify all members of the wireless LAN.
- The MAC addresses of all the wireless cards that will be used to access the 3e–525C–2 network of access points (if MAC address filtering is to be enabled)
- The appropriate encryption key for Static AES if state-of-the art key management will be used. Alternately, the appropriate WEP key.

Initial Setup using the "Local" Port

Plug one end of an RJ-45 Ethernet cable to the LAN port of the 3e–525C–2 (see page 11) and the other end to an Ethernet port on your PC/laptop. This LAN port in the 3e–525C–2 connects you to the device's internal DHCP server which will dynamically assign an IP address to your laptop so you can access the device for configuration. In order to connect properly to the 3e–525C–2 on the LAN port, the TCP/IP parameters on your laptop must be set to "obtain IP address automatically." (If you are unfamiliar with this procedure, use the following instructions for determining or changing your TCP/IP settings.)

In Windows 98/Me click **Start → Settings → Control Panel**. Find and double click the **Network** icon. In the **Network** window, highlight the TCP/IP protocol for your LAN and click the Properties button. Make sure that the radio button for **Obtain an IP address automatically** is checked.

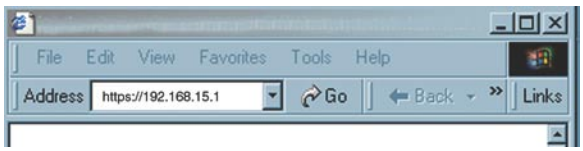
In Windows 2000/XP, follow the path **Start → Settings → Network and Dialup Connections → Local Area Connection** and select the **Properties** button. In the **Properties** window, highlight the TCP/IP protocol and click properties. Make sure that the radio button for **Obtain an IP address automatically** is checked.

Once the DHCP server has recognized your laptop and has assigned a dynamic IP address, you will need to find that IP address. Again, the procedure is similar for Windows 95/98/Me machines and slightly different for Windows 2000/XP machines.

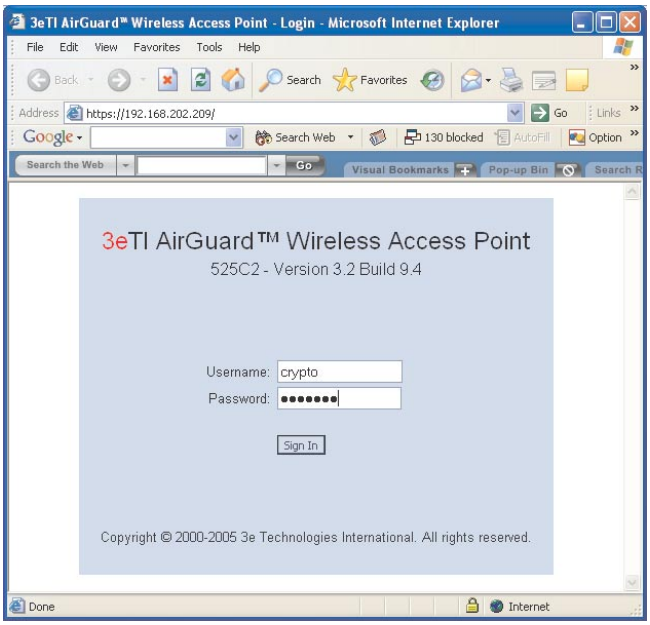
In Windows 98/Me, click **Start**, then **Run** and type **winipcfg** in the run instruction box. Then click **OK**. You will see the IP address of your laptop in the resulting window, along with the "default gateway" IP address. Verify that the IP address shown is 192.168.15.x

In Windows 2000/XP, click **Start**, then **Run** and type **cmd** in the run instruction box. Then click **OK**. This will bring up a window. In this window, type **ipconfig /all |more**. This will list information assigned to your laptop, including the IP address assigned. Verify that the IP address shown is 192.168.15.x

On your computer, pull up a browser window and put the default URL for the 3e–525C–2 Local LAN in the address line. (https://192.168.15.1)



You will be asked for your User Name and Password. The default is "crypto" with the password "officer" to give full access for setup configuration. (This password is case-sensitive.)


3eTI AirGuard™ Wireless Access Point - Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://192.168.202.209/
3eTI AirGuard™ Wireless Access Point
525C2 - Version 3.2 Build 9.4
Username: crypto
Password:
Sign In
Copyright © 2000-2005 3e Technologies International. All rights reserved.
Done
Internet

NOTE: If your login session is in-active for more than 10 minutes, then you will have to re-authenticate your identity. If after three times you fail to re-authenticate then your account will be locked. The exception is if you are the last active CryptoOfficer on the system, then your account will not be locked. The **User Management—List All Users** screen displays account status. If an account is locked, it will show a status of "Locked" and a reason of "bad passwd". Other accounts show status as "Active" and reason "Normal".

The CryptoOfficer is the only role that can unlock an account once it has been locked. Go to the **User Management—List All Users** screen and click the unlock buttn at the end of the user entry.

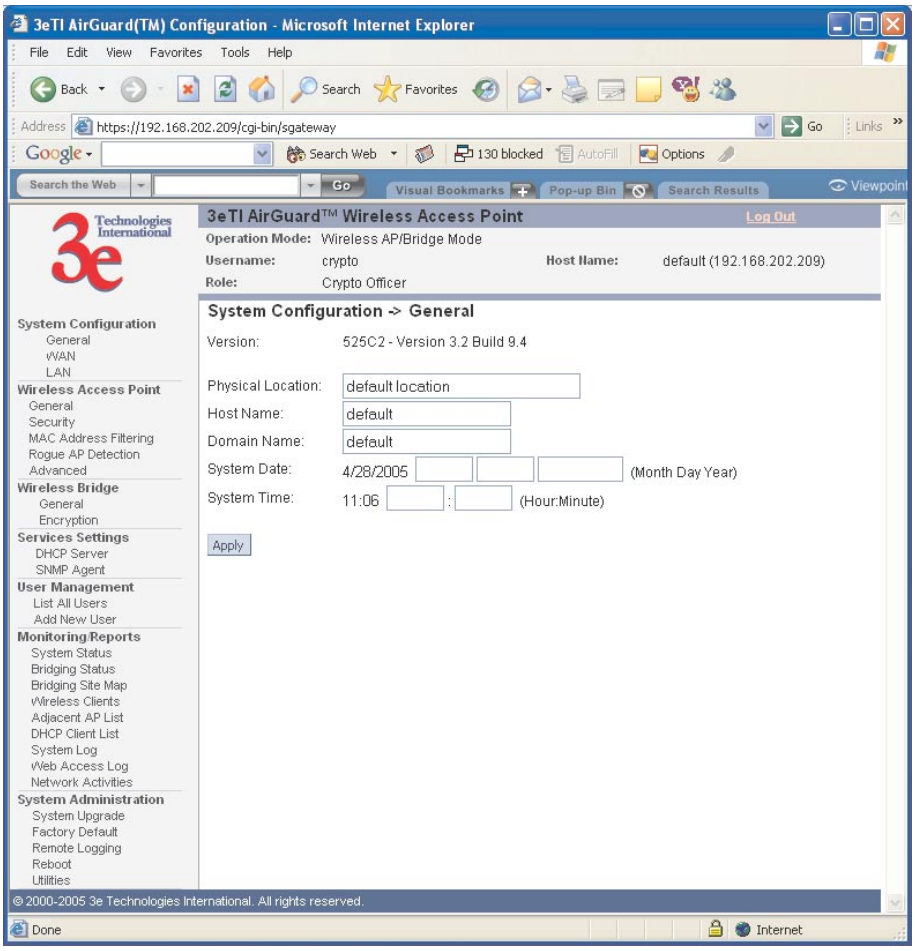
If you have forgotten your user name or password you can reset the unit back to its factory default username and password by pressing and holding the reset button on the front of the unit for 10 seconds. Note that all your settings will also be reset to factory defaults.

System Configuration

General

You will immediately be directed to the **System Configuration — General** screen for the 3e–525C–2 access point.

This screen lists the firmware version number for your 3e–525C–2 and allows you to set the Host Name and Domain Name as well as establish system date and time. (Host and Domain Names are both set at the factory for "default" but can optionally be assigned a unique name for each.) You can also enter a description of the physical location of the unit in the Physical Location field. This is useful when deploying units to remote lcoations. When you are satisfied with your changes, click **Apply**.



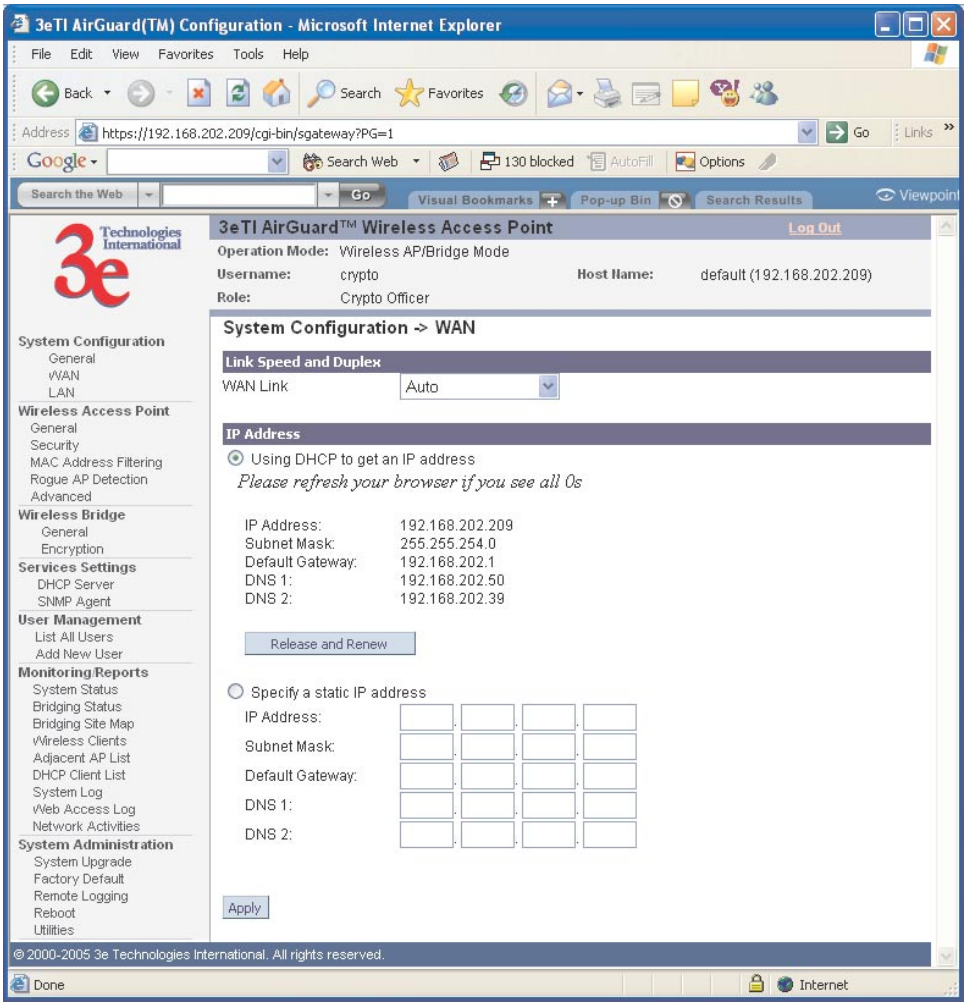
Go next to the **System Configuration — WAN** page.

WAN

Click the entry on the left hand navigation panel for **System Configuration — WAN**. This directs you to the **System Configuration — WAN** screen.

If not using DHCP to get an IP address, input the static IP information that the access point requires in order to be managed from the wired LAN. This will be the IP address, Subnet Mask, Default Gateway, and, where needed, DNS 1 and 2.

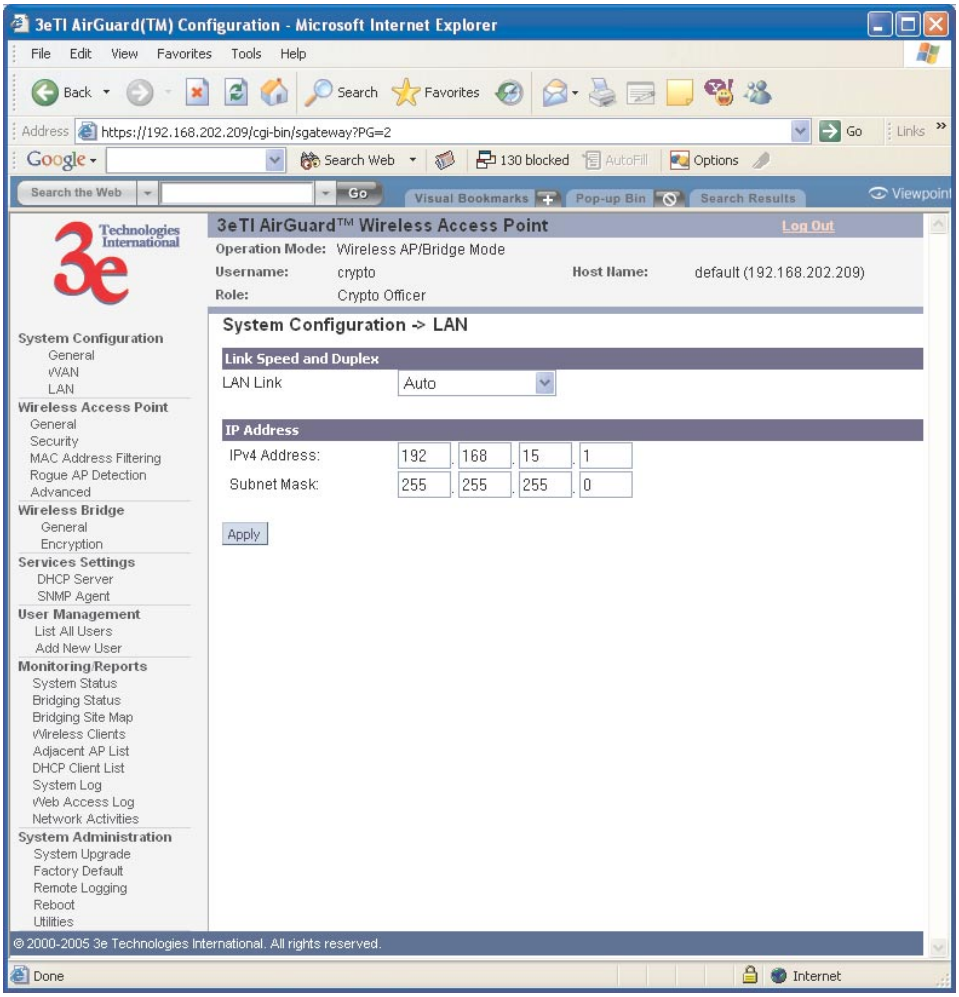
Click **Apply** to accept changes.



LAN

Click the entry on the left hand navigation panel for **System Configuration — LAN**. This directs you to the **System Configuration — LAN** screen.

This sets up the default numbers for the four octets for a possible private LAN function for the access point. It also allows changing the default numbers for the LAN Subnet Mask. The Local LAN port provides local access for configuration. It is not advisable to change the private LAN address while doing the initial setup as you are connected to that LAN.



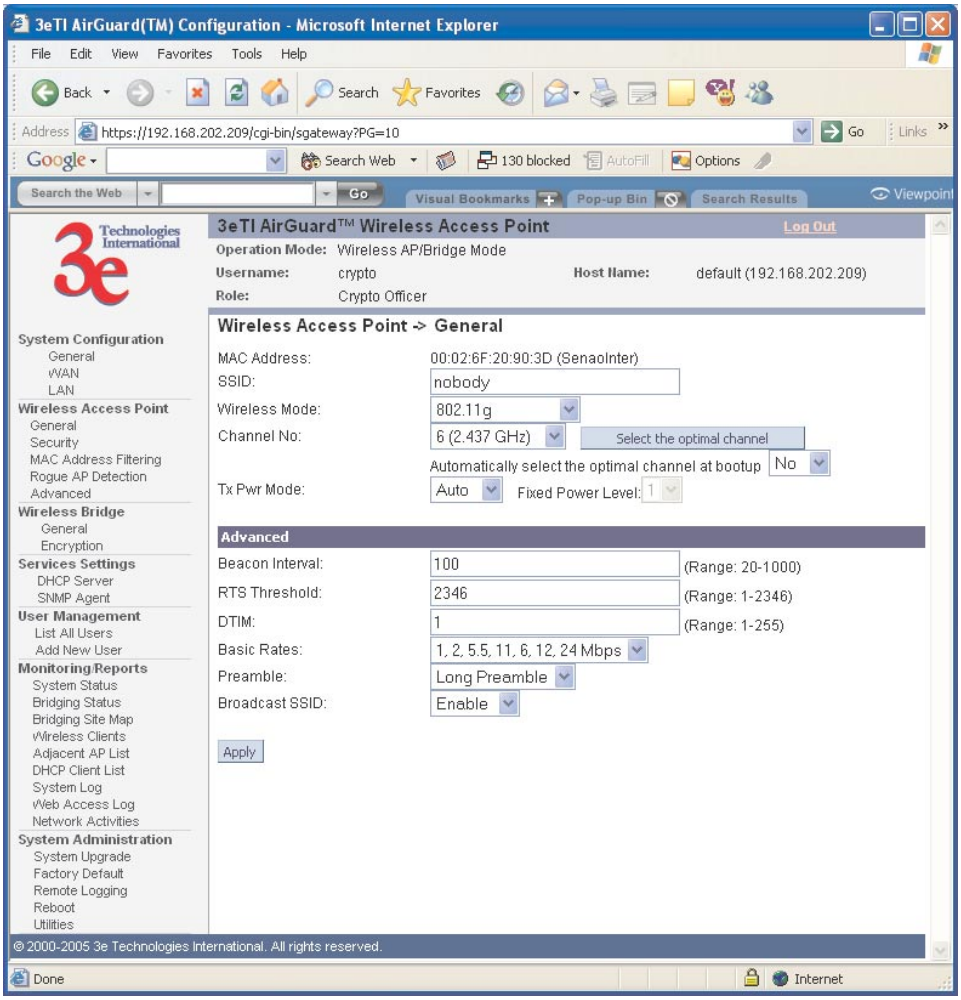
Wireless Access Point Configuration

General

Wireless Setup allows your computer's PC Card to communicate with the access point. Follow the manufacturer's instructions to set up the PC Card on each wireless device that will be part of the WLAN.

The **Wireless Access Point — General** screen lists the MAC Address of the AP card. This is not the MAC Address that will be used for the BSSID for bridging setup, however. That is found on the **Wireless Bridge — General** screen.

If you will be using an **SSID** for a wireless LAN, enter it here and in the setup of each wireless client. This nomenclature has to be set on the access point and each wireless device in order for them to communicate.



Select the wireless mode from the drop-down list. You can choose from the following options:

- 802.11b
- 802.11g
- 802.11g Super
- 802.11b/g Mixed
- 802.11a
- 802.11a Turbo

You can assign a channel number to the AP (if necessary) and modify the Tx Pwr Mode.

The **Channel Number** is a means of assigning frequencies to a series of access points, when many are used in the same WLAN, to minimize noise. There are 11 channel numbers that may be assigned. If you assign channel number 1 to the first in a series, then channel 6, then channel 11, and then continue with 1, 6, 11, you will have the optimum frequency spread to decrease "noise."

If you click on the button **Select the optimal channel**, a popup screen will display the choices. It will select the optimal channel for you. You can also set it up to automatically select the optimal channel at boot up.

CHANNEL NO. OPTIONS	
Wireless Mode	**Channel No.**
802.11b **802.11g** **802.11b/g Mixed**	1 (2.412 GHz) 2 (2.417 GHz) 3 (2.422 GHz) 4 (2.427 GHz) 5 (2.432 GHz) 6 (2.437 GHz) 7 (2.442 GHz) 8 (2.447 GHz) 9 (2.452 GHz) 10 (2.457 GHz) 11 (2.462 GHz)
802.11g Super	6 (2.437 GHz)
802.11a	52 (5.26 GHz) 56 (5.28 GHz) 60 (5.30 GHz) 64 (5.32 GHz) 149 (5.745 GHz) 153 (5.765 GHz) 157 (5.785 GHz) 161 (5.805 GHz) 165 (5.825 GHz)
802.11a Turbo	50 (5.25 GHz) Turbo Mode 58 (5.29 GHz) Turbo Mode 152 (5.76 GHz) Turbo Mode 160 (5.80 GHz) Turbo Mode

Tx Pwr Mode and Fixed Pwr Level: The Tx Power Mode defaults to Auto, giving the largest range of radio transmission available under normal conditions. As an option, the AP's broadcast range can be limited by setting the Tx Power Mode to Fixed and choosing from 1-5 for Fixed Pwr Level (1 being the shortest distance.) Finally, if you want to prevent any radio frequency transmission, set Tx Pwr Mode to **Off**.

There are a number of advanced options included on this page as described in the following chart:

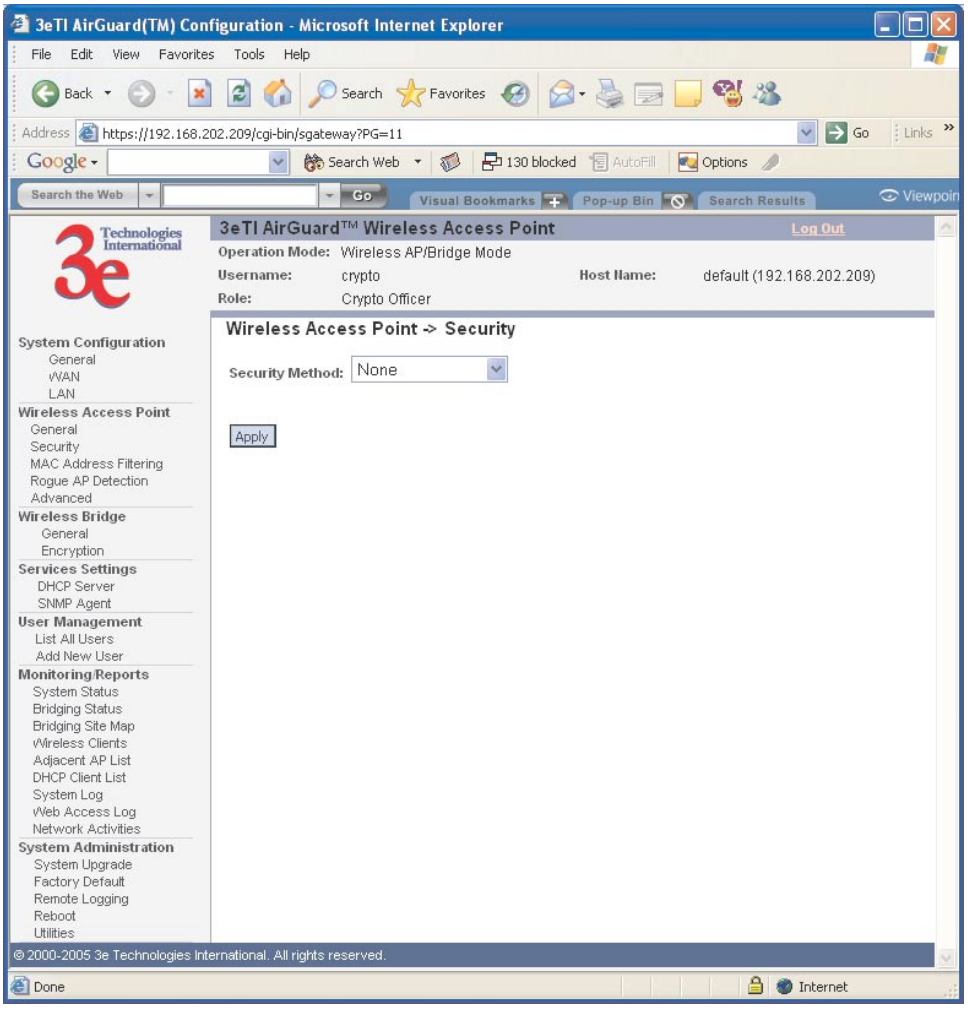
ADVANCED OPTIONS		
Beacon interval	20-1000	The time interval in milliseconds in which the 802.11 beacon is transmitted by the AP.
RTS Threshold	1-2346	The number of bytes used for the RTS/CTS handshake boundary. When a packet size is greater than the RTS threshold, the RTS/CTS handshaking is performed.
DTIM	1-255	The number of beacon intervals that broadcast and multicast traffic is buffered for a client in power save mode.
Basic Rates	**Basic Rates for 802.11b**	
	1 and 2 Mbps 1, 2, 5.5 and 11 Mbps	The basic rates used and reported by the AP. The highest rate specified is the rate that the AP uses when transmitting broadcast/multicast and management frames.
	Basis Rates for 802.11g	
	1, 2, 5.5, 11, 6, 12, 24 Mbps 1, 2, 5.5, 11 Mbps	
	Basic Rates for 802.11g Super	
	1, 2, 5.5, 11, 6, 12, 24 Mbps 1, 2, 5.5, 11 Mbps	
	Basic Rates for 802.11b/g Mixed	
	1, 2 Mbps 1, 2, 5.5, 11 Mbps	
	Basic Rates for 802.11a	
	6, 12, 24 Mbps	
	Basic Rates for 802.11a Turbo	
	6, 12, 24 Mbps	
Preamble	Short/Long Preamble	Specifies whether frames are transmitted with the Short or Long Preamble
Broadcast SSID	Enabled/disabled	When disabled, the AP hides the SSID in outgoing beacon frames and stations cannot obtain the SSID through passive scanning. Also, when it is disabled, the AP doesn't send probe responses to probe requests with unspecified SSIDs.

Security

The **Wireless Access Point — Security** screen displays a default factory setting of no encryption, but for security reasons it will not communicate to any clients unless the encryption is set by the CryptoOfficer.

No Encryption

In order to have the 3e–525C–2 work with no encryption, you must actively select **None** and click **Apply**. A screen will appear, asking if you really want to operate in Bypass mode. If you answer **Yes**, no encryption will be applied.

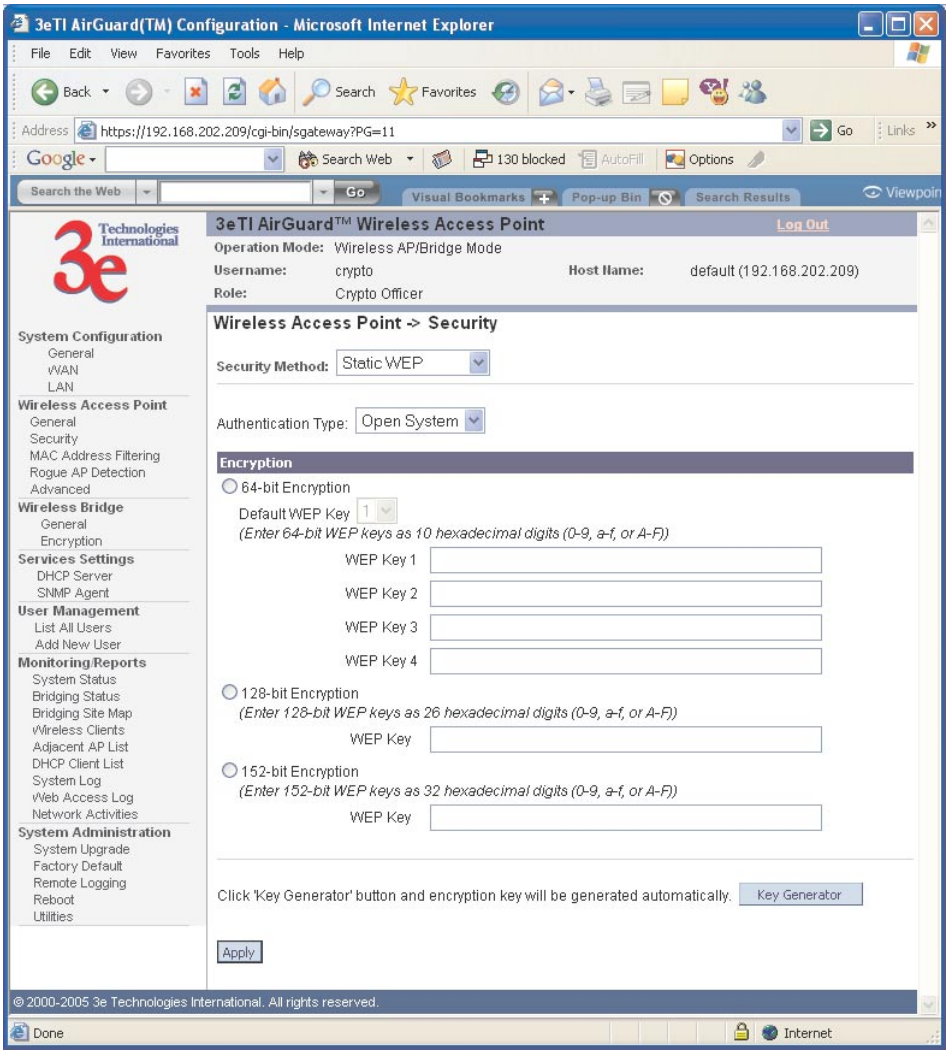


Static WEP Encryption

If you choose to use WEP encryption, you can also select whether it will be Open System or Shared Key authentication. For greater security, set authentication type to “shared key.” WEP Data encryption can be set to 64-bit, 128-bit, or 152-bit encryption.

The Key Generator button automatically generates a randomized key of the appropriate length. This key is initially shown in plain text so the user has the opportunity to copy the key. Once the key is applied, the key is no longer displayed in plain text.

WEP (**W**ired **E**quivalent **P**rivacy) Encryption is a security protocol for wireless local area networks (WLANs) defined in the IEEE 802.11 standard. WEP was originally designed to provide the same level of security for wireless LANs as that of a wired LAN but has come under attack for its defaults and is not now state of the art. WEP relies on the use of identical static keys deployed on client stations and access points. But the use of WEP encryption provides some measure of security.



Utilities exist for scanning for networks and logging all the networks it runs into—including the real SSIDs, the access point's MAC address, the best signal-to-noise ratio encountered, and the time the user crossed into the network's space. These utilities can be used to determine whether your network is unsecured. Note that, if WEP is enabled, that same WEP key must also be set on each wireless device that is to become part of the wireless network, and, if "shared key" is accepted, then each wireless device must also be coded for "shared key". To use WEP encryption, identify the level of encryption, the Default WEP key and designate the WEP keys as shown on the screen.

802.11i and WPA

Wi-Fi Protected Access or WPA was designed to enable use of wireless legacy systems employing WEP while improving security. WPA uses improved data encryption through the temporal key integrity protocol (TKIP) which scrambles keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. In addition, user authentication is enabled using the extensible authentication protocol (EAP).

If you wish to use WPA on the 3e–525C–2, enable either WPA Pre-shared Key Settings or WPA 802.1x Settings.

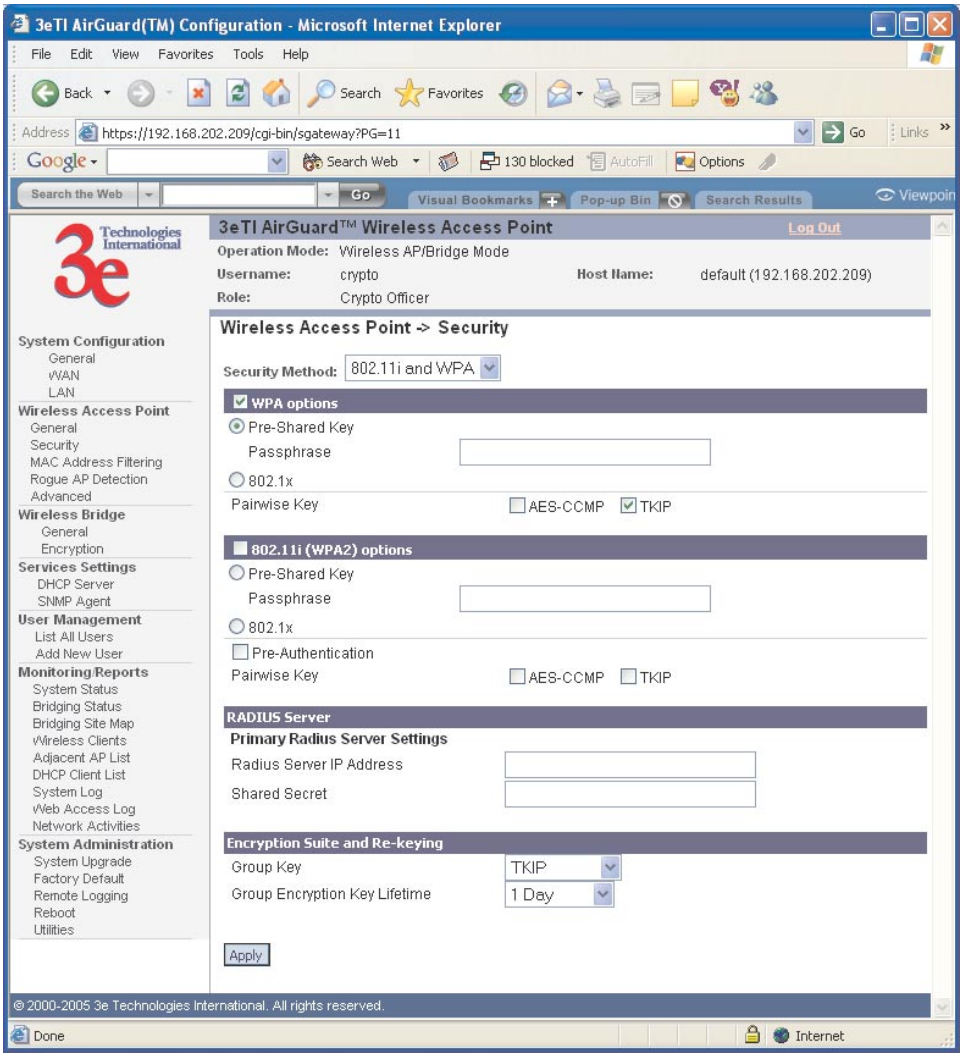
If you are a SOHO user, selecting pre-shared key means that you don't have the expense of installing a Radius Server. Simply input up to 63 character / numeric / hexadecimals in the Passphrase field. If your clients use WPA-TKIP, select TKIP as encryption type. If your clients use WPA-AES, select AES-CCMP.

Enable pre-authentication to allow a client to authenticate in advance with the AP before the client is associated with it. Allowing the AP to pre-authenticate a client decreases the transition time when a client roams between APs.

Re-keying time is the frequency in which new encryption keys are generated and distributed to the client. The more frequent re-keying, the better the security. For highest security, select the lowest re-keying interval.

As an alternative, for business applications who have installed Radius Servers, select WPA 802.1x and input the Primary and Backup Radius Server settings. Use of Radius Server for key management and authentication requires that you have installed a separate certification system and each client must have been issued an authentication certificate.

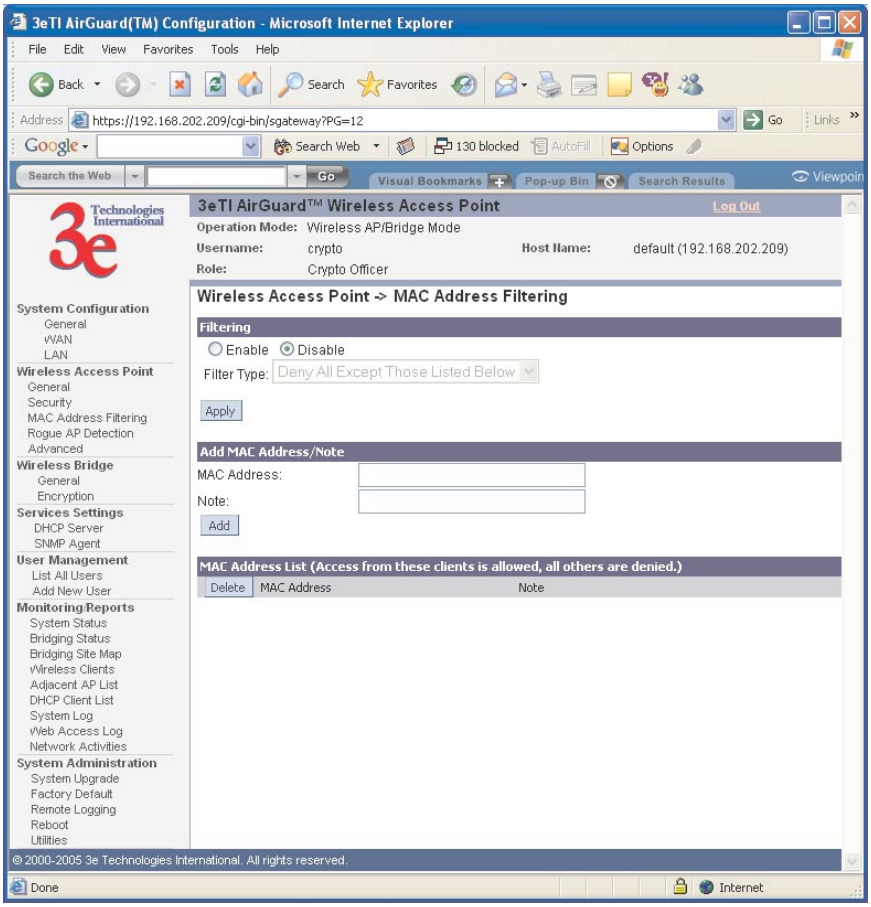
Once you have selected the options you will use, click **Apply**.



If you will be using MAC Address filtering, navigate next to the MAC Address Filtering screen.

MAC Address Filtering

The **Wireless Access Point — MAC Address Filtering** screen is used to set up MAC address filtering for the 3e–525C–2 device. The factory default for MAC Address filtering is **Disabled**. If you enable MAC Address filtering, you should also set the toggle for **Filter Type**.



This works as follows:

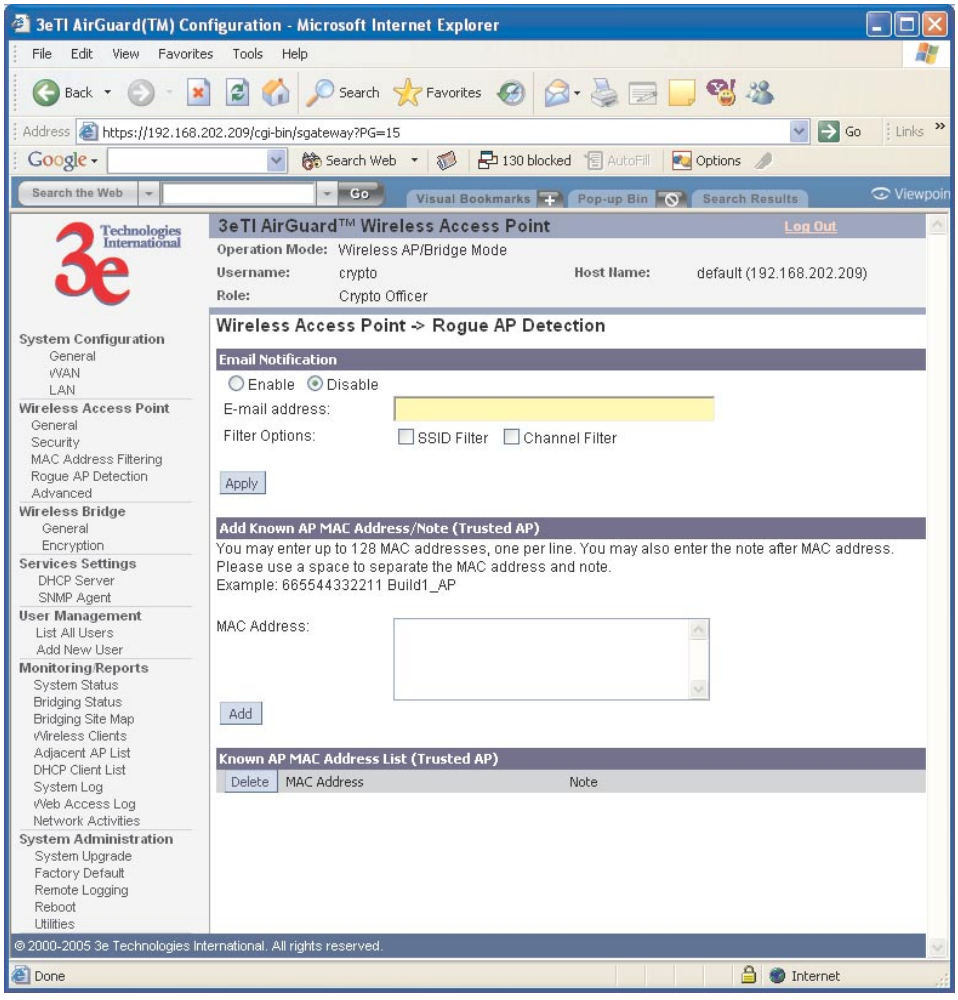
- If **Filtering** is enabled and **Filter Type** is **Deny All Except Those Listed Below**, only those devices equipped with the authorized MAC addresses will be able to communicate with the access point. In this case, input the MAC addresses of all the PC cards that will be authorized to access this access point. The MAC address is engraved or written on the PC (PCMCIA) Card.
- If **Filtering** is enabled and **Filter Type** is **Allow All Except Those Listed Below**, those devices with a MAC address which has been entered in the MAC Address listing will NOT be able to communicate with the access point. In this case, navigate to the report: **Wireless Clients** and copy the MAC address of any Wireless Client that you want to exclude from communication with the access point and input those MAC Addresses to the MAC Address list.

Rogue AP Detection

The **Wireless Access Point — Rogue AP Detection** screen allows the network administrator to set up rogue AP detection. Enable rogue AP detection and enter the MAC Address of each AP in the network that you want the AP being configured to accept as a trusted AP. (You may add up to 20 APs.) Enter an email address for notification of any rogue or non-trusted APs. (The MAC Address for the 3e–525C–2 is located on the **System Configuration — General** screen. You can also select the following filter options.

- **SSID FIlter**: Check the SSID option to only send rogue APs that match the AP's SSID or wireless bridge's SSID.
- **Channel Filter**: Check the channel filter option to only send rogue APs that match the AP's channel or the wireless bridge's channel.
- If both options are checked, only APs that match both the SSID and channel are sent.

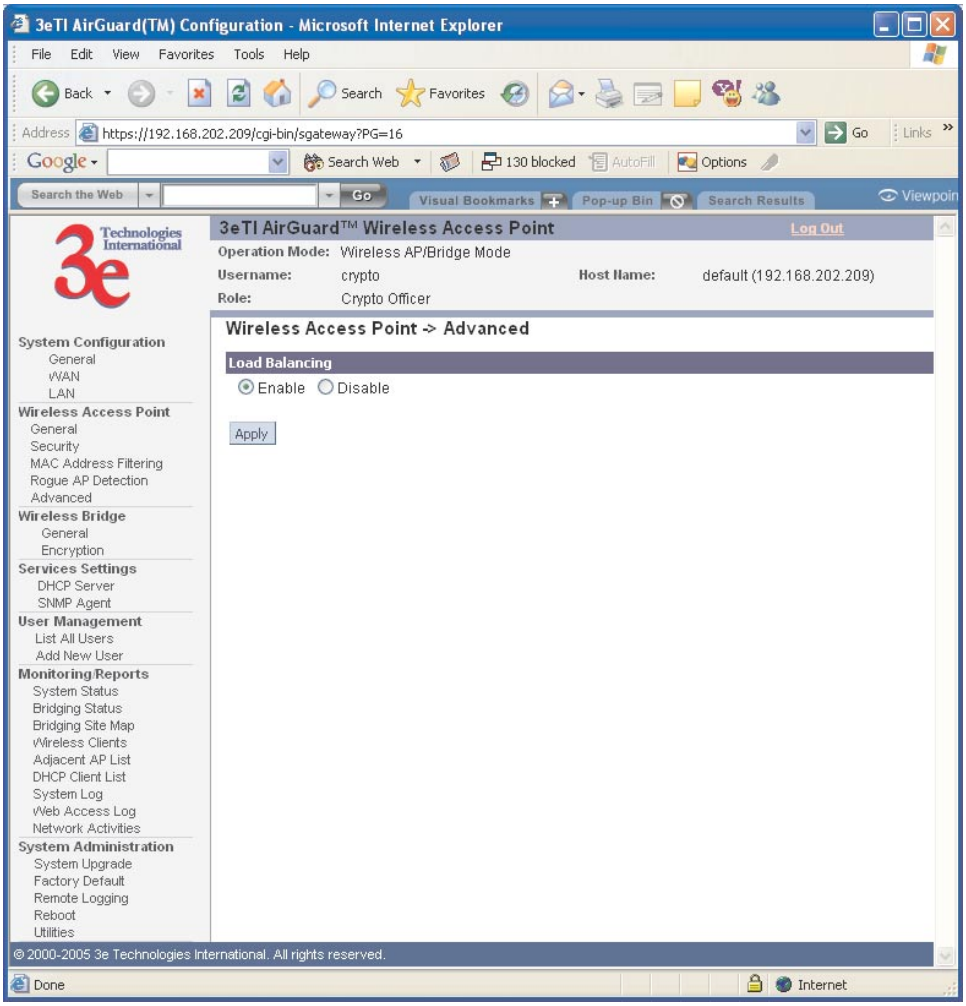
The **Adjacent AP list**, under **Monitoring/Reports** on the navigation menu, will detail any marauding APs.



Advanced

The **Wireless Access Point — Advanced** screen allows you to enable or disable load balancing and to control bandwidth.

Load balancing is enabled by default. The load balancing feature balances the wireless clients between APs. If two APs with similar settings are in a conference room, depending on the location of the APs, all wireless clients could potentially associate with the same AP, leaving the other AP unused. Load balancing attempts to evenly distribute the wireless clients on both APs.



Once you have made any changes, click **Apply** to save.

Wireless Bridge

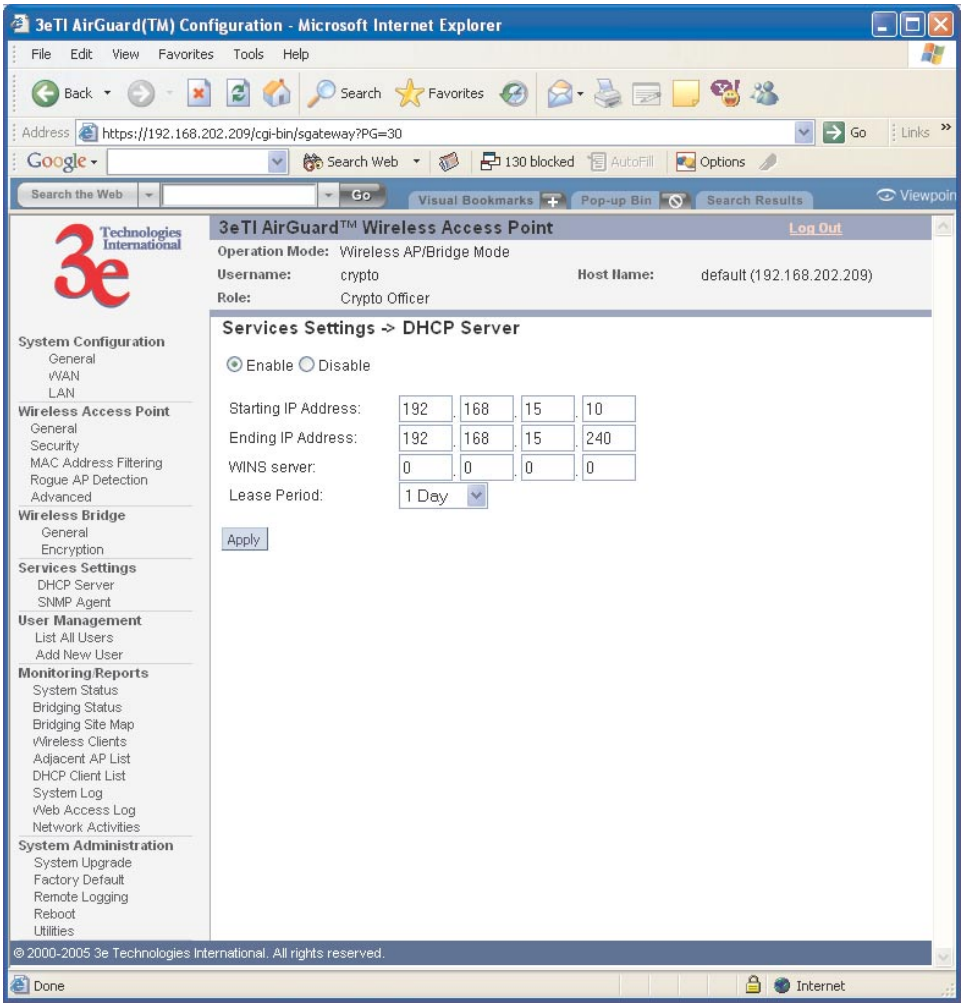
The Wireless Bridge screens are described in Chapter 4.

Services Settings

DHCP Server

The **Service Settings — DHCP Server** screen is used for configuring the DHCP server function accessible from the Local LAN port. The default factory setting for the DHCP server function is enabled. You can disable the DHCP server function, if you wish, but it is not recommended. You can also set the range of addresses to be assigned. The Lease period (after which the dynamic address can be reassigned) can also be varied.

The DHCP server function, accessible only from the LAN port, is used for initial configuration of the management functions.

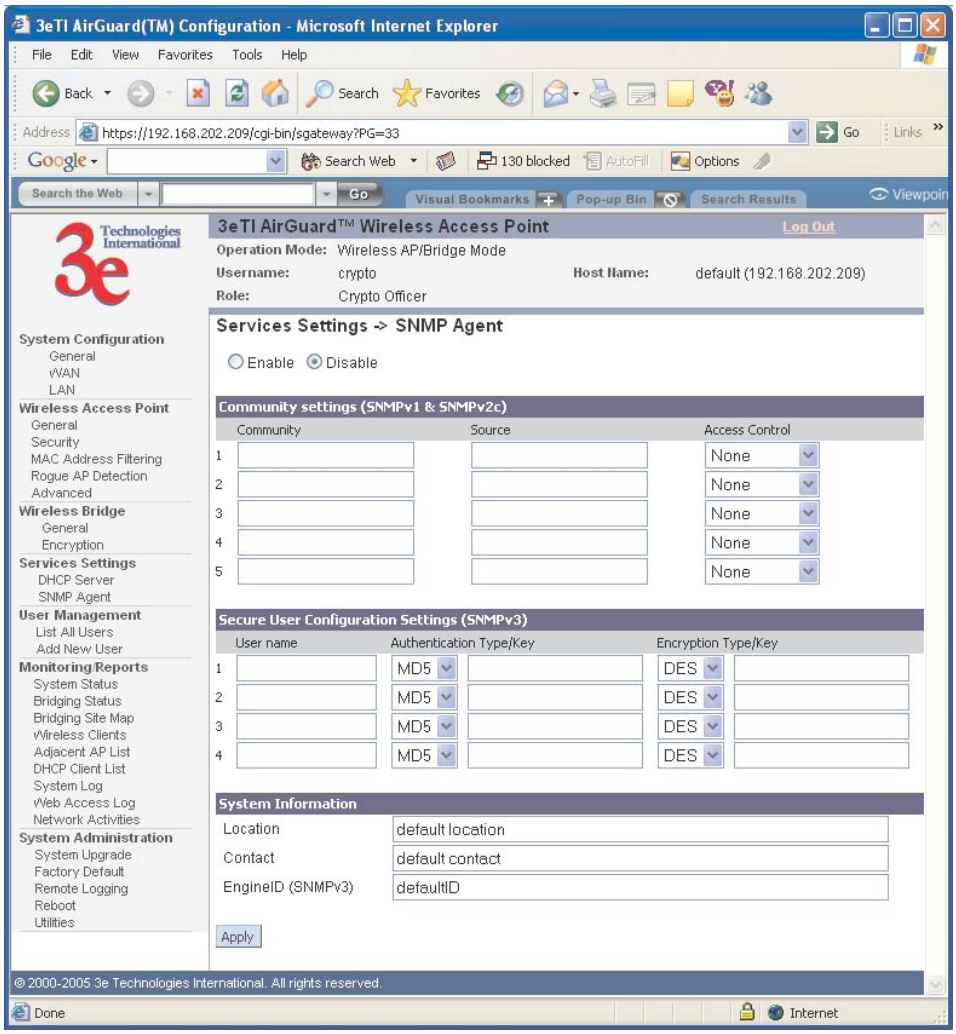


SNMP Agent

The **Service Settings — SNMP Agent** screen allows you to set up an SNMP Agent. The agent is a software module that collects and stores management information for use in a network management system. The 3e–525C–2's integrated SNMP agent software module translates the device's management information into a common form for interpretation by the SNMP Manager, which usually resides on a network administrator's computer.

The SNMP Manager function interacts with the SNMP Agent to execute applications to control and manage object variables (interface features and devices) in the gateway. Common forms of managed information include number of packets received on an interface, port status, dropped packets, and so forth. SNMP is a simple request and response protocol, allowing the manager to interact with the agent to either:

- **Get** - Allows the manager to **Read** information about an object variable
- **Set** - Allows the manager to **Write** values for object variables within an agent's control, or



The SNMP configuration consists of several fields, which are explained below:

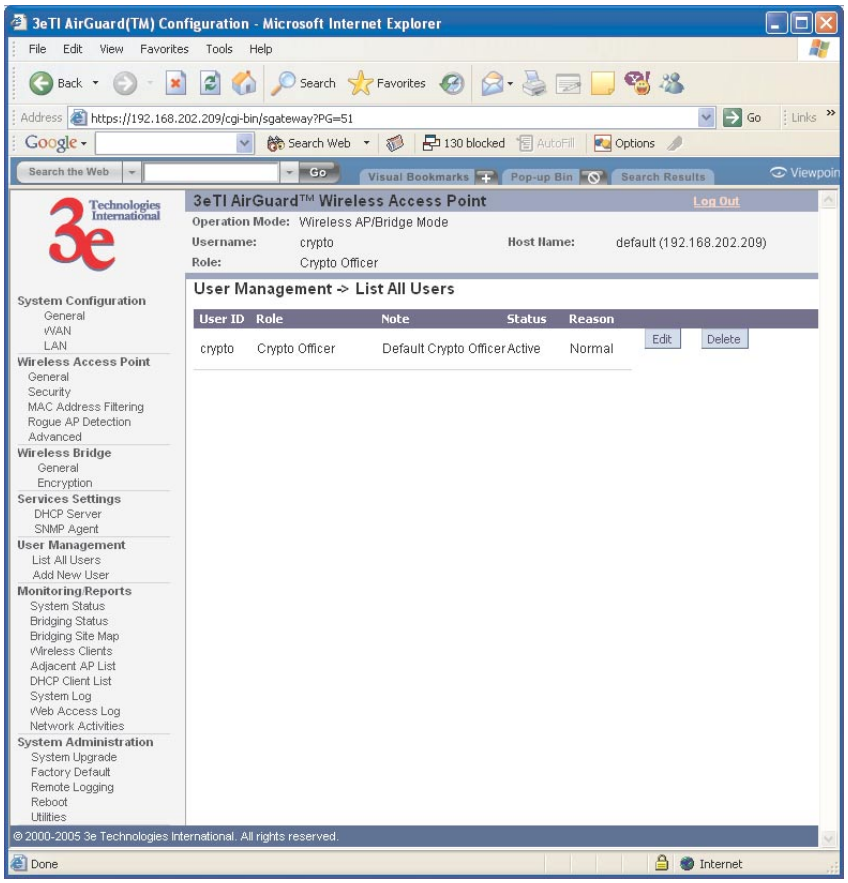
- **Community** –The Community field for Get (Read Only), Set (Read & Write), and Trap is simply the SNMP terminology for "password" for those functions.
- **Source** –The IP address or name where the information is obtained.
- **Access Control** –Defines the level of management interaction permitted.

If using SNMPv3, enter a username (minimum of eight characters), authentication type with key and data encryption type with a key. This configuration information will also need to be entered in your MIB manager setup.

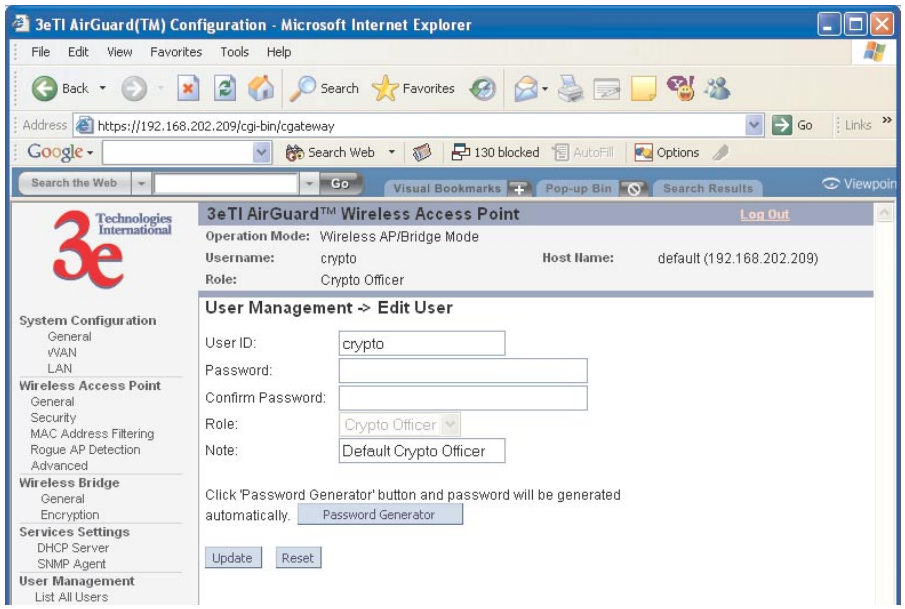
User Management

List All Users

The **User Management — List All Users** screen lists the Crypto Officer and administrator accounts configured for the unit. You can edit or delete users from this screen.



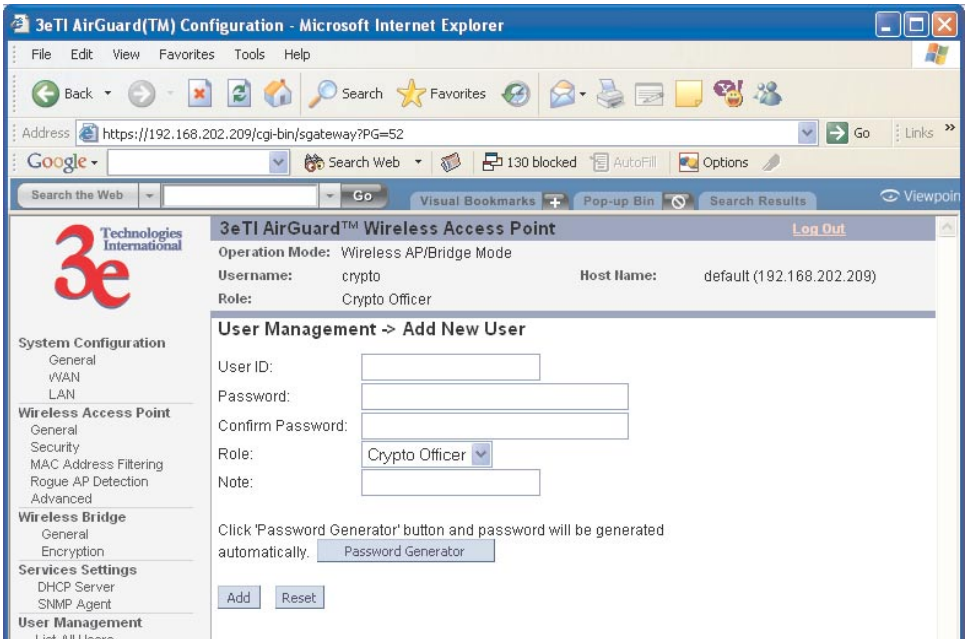
If you click on Edit, the **User Management — Edit User** screen appears. On this screen you can edit the user ID, password, role, and note fields.



The **Password Generator** button creates a random password so that you don't need to create one. Initially, the password is shown in plain text so that you can copy it. Once the **Apply** button is pressed, the password is no longer shown.

Add New User

The **User Management — Add New User** screen allows you to add new Administrators and CryptoOfficers, assigning and confirming the password.

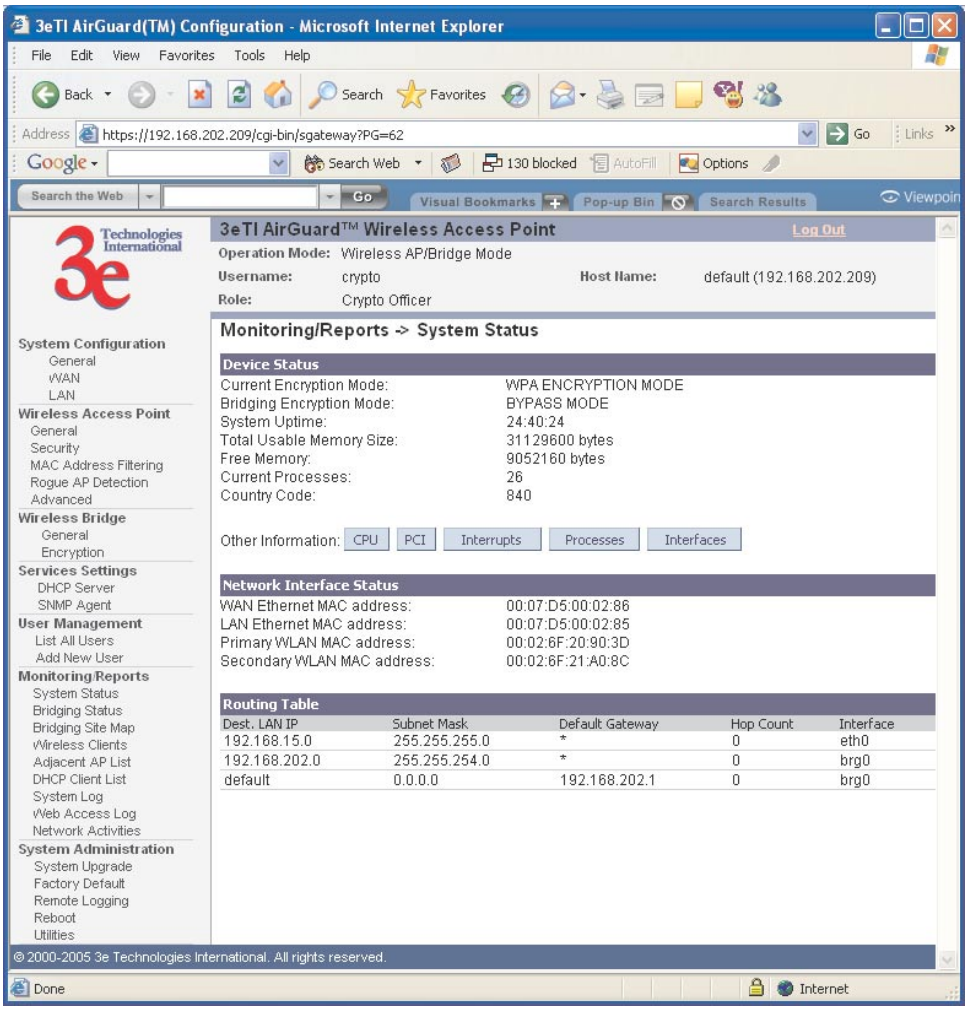


Monitoring/Reports

This section gives you a variety of lists and status reports. Most of these are self-explanatory.

System Status

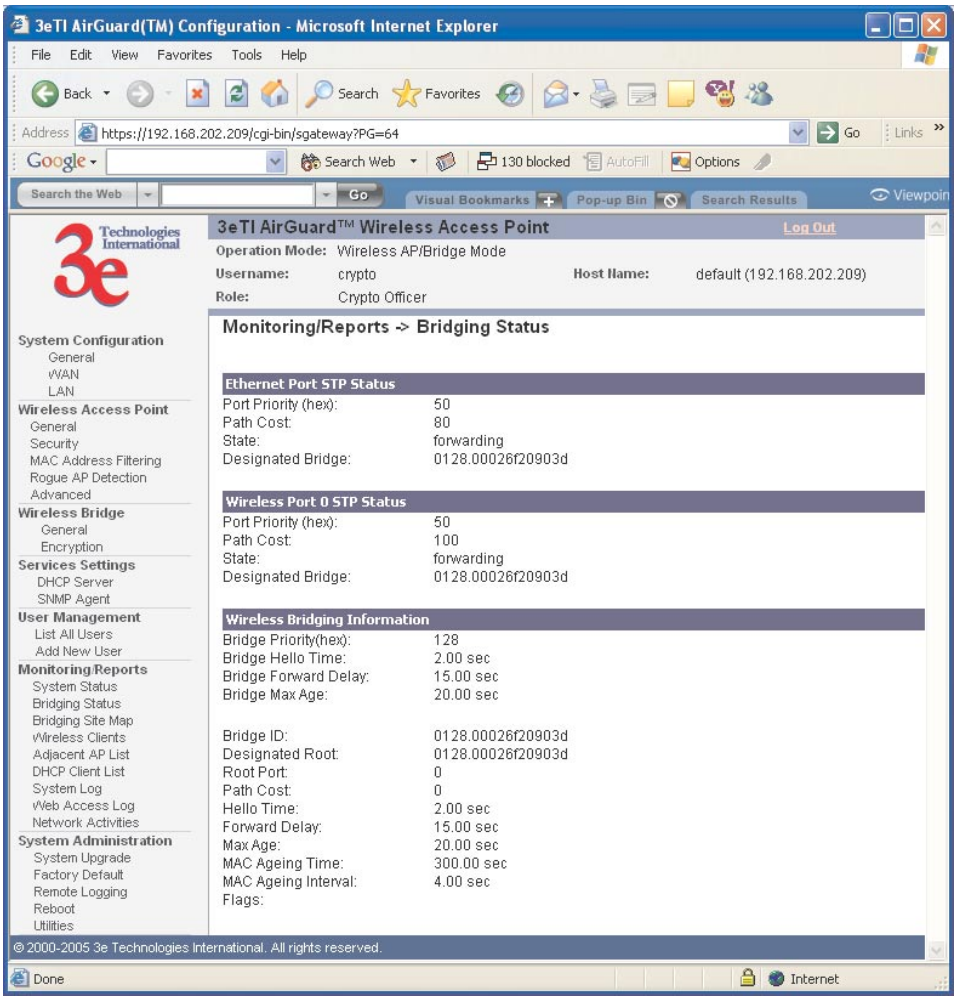
The **Monitoring/Report — System Status** screen displays the status of the 3e–525C–2 device, the network interface, and the routing table.



There are some pop-up informational menus that give detailed information about **CPU, PCI, Interrupts, Process,** and **Interfaces**.

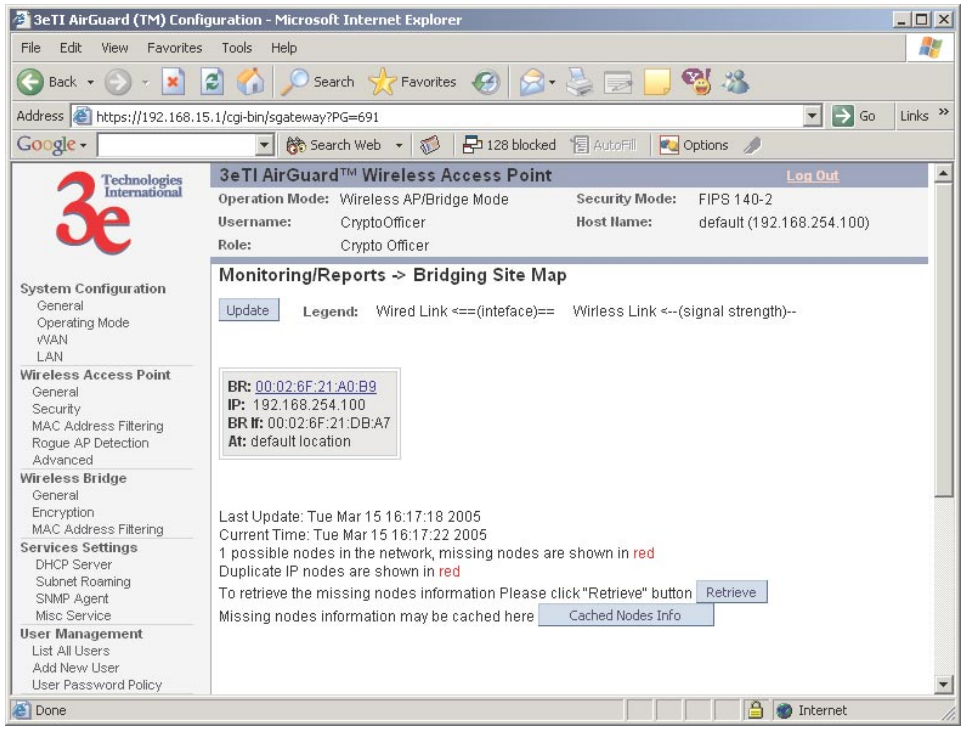
Bridging Status

The **Monitoring/Report — Bridging Status** screen displays the Ethernet Port STP status, Ethernet DSL Port STP status, Wireless Port STP status, and Wireless Bridging information.



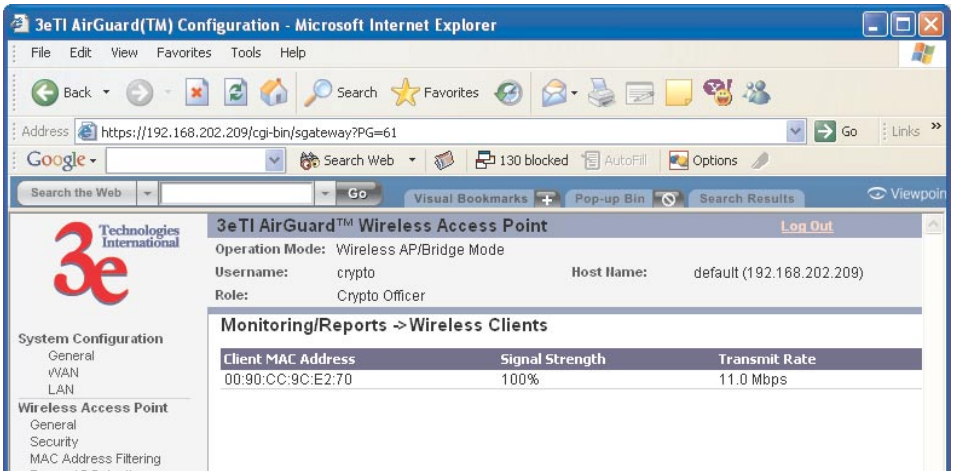
Bridge Site Map

The Bridge Site Map shows the spanning tree network topology of both wired and wireless nodes connected to the network. The root STP node is always on top and the nodes of the hierarchy are displayed below it. Wired links are double dotted lines and wireless links are single dotted lines. This map does not update dynamically. You must press the Update button to refresh the map.



Wireless Clients

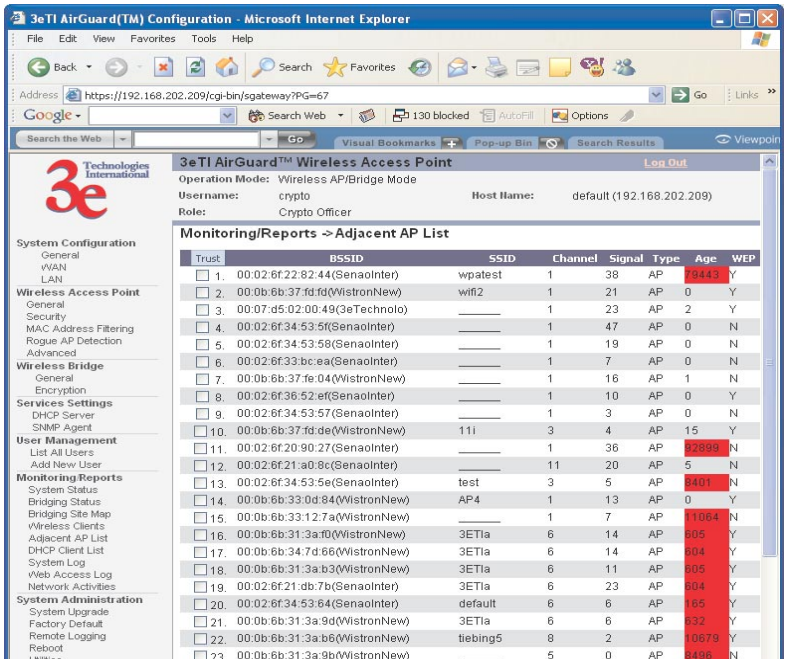
The **Monitoring/Report — Wireless Clients** screen displays the MAC Address of all wireless clients and their signal strength and transmit rate.



Adjacent AP List

The **Monitoring/Report — Adjacent AP List** screen shows all the APs on the network. If you select the check box next to any AP shown, the AP will thereafter be accepted by the 3e–525C–2 as a trusted AP.

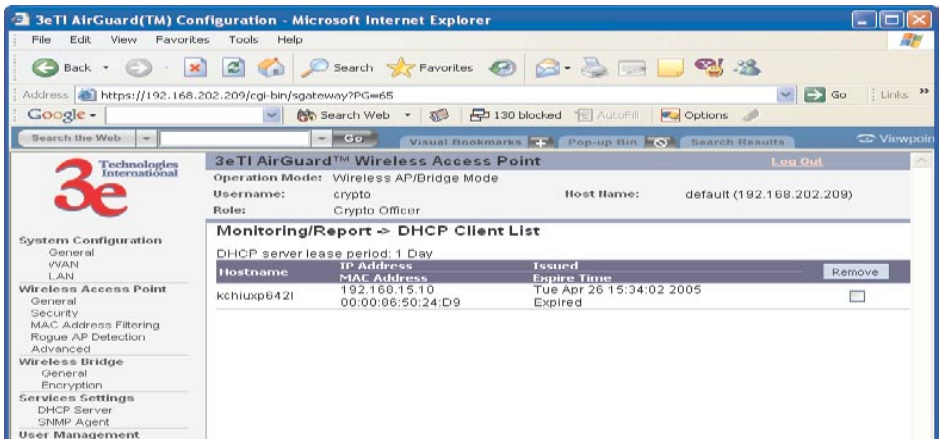
These APs are detected by the AP's wireless card (2.4 GHz band) and the wireless bridge's wireless card (5.8GHz band). The list of APs are only within the band that can be seen from a particular channel. For example, if the AP is on channel 1, it will display APs on channels 1-3.


3eTI AirGuard(TM) Configuration - Microsoft Internet Explorer
https://192.168.202.209/cgi-bin/sgateway?PG=67
3eTI AirGuard™ Wireless Access Point
Log Out
Operation Mode: Wireless AP/Bridge Mode
Username: crypto
Host Name: default (192.168.202.209)
Role: Crypto Officer
Monitoring/Reports ->Adjacent AP List
Trust
BSSID
SSID
Channel
Signal
Type
Age
WEP
1. 00:02:6f:22:82:44(SenaoInter) wpatest 1 38 AP 79443 Y
2. 00:0b:6b:37:fd:fd(WistronNew) wifi2 1 21 AP 0 Y
3. 00:07:d5:02:00:49(3eTechnolo) 1 23 AP 2 Y
4. 00:02:6f:34:53:5f(SenaoInter) 1 47 AP 0 N
5. 00:02:6f:34:53:58(SenaoInter) 1 19 AP 0 N
6. 00:02:6f:33:bc:ea(SenaoInter) 1 7 AP 0 N
7. 00:0b:6b:37:fe:04(WistronNew) 1 16 AP 1 N
8. 00:02:6f:36:52:ef(SenaoInter) 1 10 AP 0 Y
9. 00:02:6f:34:53:57(SenaoInter) 1 3 AP 0 N
10. 00:0b:6b:37:fd:de(WistronNew) 11i 3 4 AP 15 Y
11. 00:02:6f:20:90:27(SenaoInter) 1 36 AP 92899 N
12. 00:02:6f:21:a0:8c(SenaoInter) 11 20 AP 5 N
13. 00:02:6f:34:53:5e(SenaoInter) test 3 5 AP 8401 N
14. 00:0b:6b:33:0d:84(WistronNew) AP4 1 13 AP 0 Y
15. 00:0b:6b:33:12:7a(WistronNew) 1 7 AP 11064 N
16. 00:0b:6b:31:3a:f0(WistronNew) 3ETIa 6 14 AP 605 Y
17. 00:0b:6b:34:7d:66(WistronNew) 3ETIa 6 14 AP 604 Y
18. 00:0b:6b:31:3a:b3(WistronNew) 3ETIa 6 11 AP 605 Y
19. 00:02:6f:21:db:7b(SenaoInter) 3ETIa 6 23 AP 604 Y
20. 00:02:6f:34:53:64(SenaoInter) default 6 6 AP 165 Y
21. 00:0b:6b:31:3a:9d(WistronNew) 3ETIa 6 6 AP 632 Y
22. 00:0b:6b:31:3a:b6(WistronNew) tiebing5 8 2 AP 10679 Y
System Configuration
Wireless Access Point
Wireless Bridge
Services Settings
User Management
Monitoring/Reports
System Administration

DHCP Client List

The **Monitoring/Report — DHCP Client List** screen displays all clients currently connected to the 3e–525C–2 via DHCP server, including their hostnames, IP addresses, and MAC Addresses.

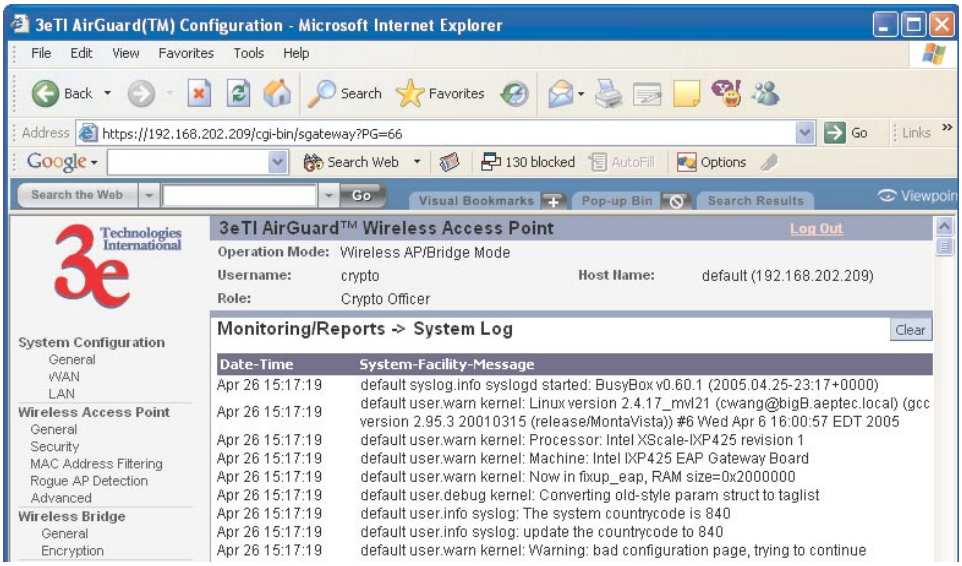
The DHCP Client list constantly collects entries. To remove entries from the list, check mark the **Revoke Entry** selection and click **Remove** to confirm the action.



System Log

The **Monitoring/Report — System Log** screen displays system facility messages with date and time stamp. These are messages documenting functions performed internal to the system, based on the system's functionality. Generally, the Administrator would only use this information if trained as or working with a field engineer or as information provided to technical support.

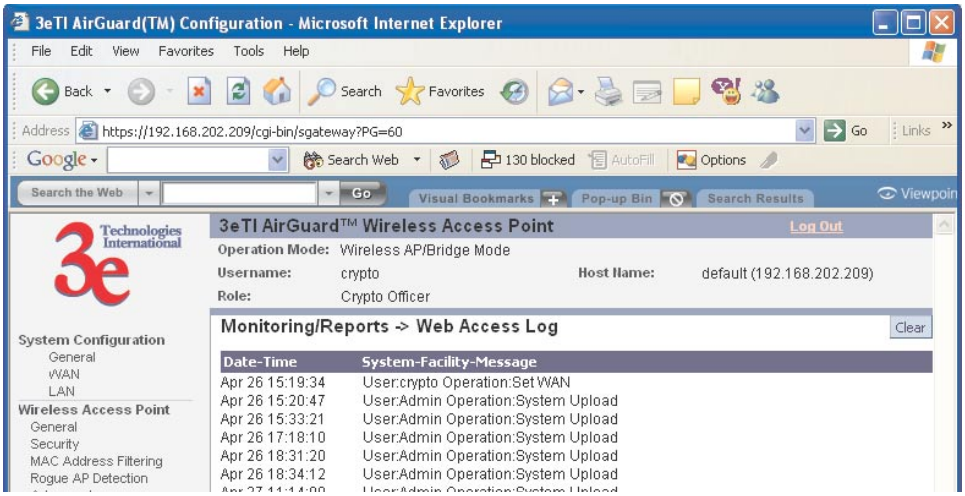
The System log continues to accumulate listings. If you wish to clear listings manually, use the **Clear** button.


3eTI AirGuard(TM) Configuration - Microsoft Internet Explorer
3eTI AirGuard™ Wireless Access Point
Log Out
Operation Mode: Wireless AP/Bridge Mode
Username: crypto
Host Name: default (192.168.202.209)
Role: Crypto Officer
Monitoring/Reports -> System Log
Clear
Date-Time
System-Facility-Message
Apr 26 15:17:19 default syslog.info syslogd started: BusyBox v0.60.1 (2005.04.25-23:17+0000)
Apr 26 15:17:19 default user.warn kernel: Linux version 2.4.17_mvl21 (cwang@bigB.aeptec.local) (gcc version 2.95.3 20010315 (release/MontaVista)) #6 Wed Apr 6 16:00:57 EDT 2005
Apr 26 15:17:19 default user.warn kernel: Processor: Intel XScale-IXP425 revision 1
Apr 26 15:17:19 default user.warn kernel: Machine: Intel IXP425 EAP Gateway Board
Apr 26 15:17:19 default user.warn kernel: Now in fixup_eap, RAM size=0x2000000
Apr 26 15:17:19 default user.debug kernel: Converting old-style param struct to taglist
Apr 26 15:17:19 default user.info syslog: The system countrycode is 840
Apr 26 15:17:19 default user.info syslog: update the countrycode to 840
Apr 26 15:17:19 default user.warn kernel: Warning: bad configuration page, trying to continue
System Configuration
General
WAN
LAN
Wireless Access Point
General
Security
MAC Address Filtering
Rogue AP Detection
Advanced
Wireless Bridge
General
Encryption

Web Access Log

The Web Access Log displays system facility messages with date and time stamp for any actions involving web access. For example, this log records when you set encryption mode, change operating mode, etc., using the web browser. It establishes a running record regarding what actions were performed and by whom.

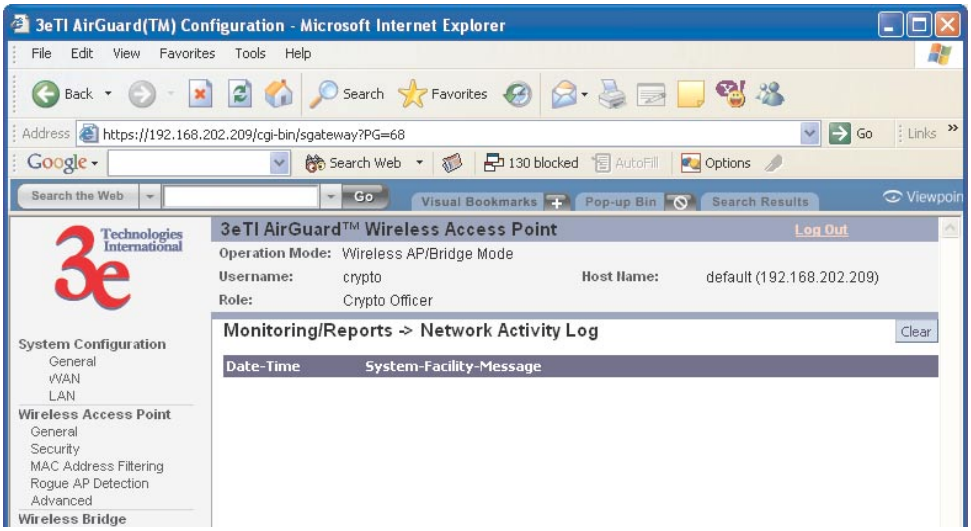
The Web access log will continue to accumulate listings. If you wish to clear listings manually, use the **Clear** button.



Network Activity

The Network Activity Log keeps a detailed log of all activities on the network which can be useful to the network administration staff.

The Network Activities log will continue to accumulate listings. If you wish to clear listings manually, use the **Clear** button.



System Administration

The System administration screens contain administrative functions. The screens and functions are detailed in the following section.

System Upgrade

The **System Administration — System Upgrade** screen gives you the ability to upload updates to the 3e–525C–2 device's firmware as they become available. When a new upgrade file becomes available, you can do a firmware upgrade from the **Firmware Upgrade** window.

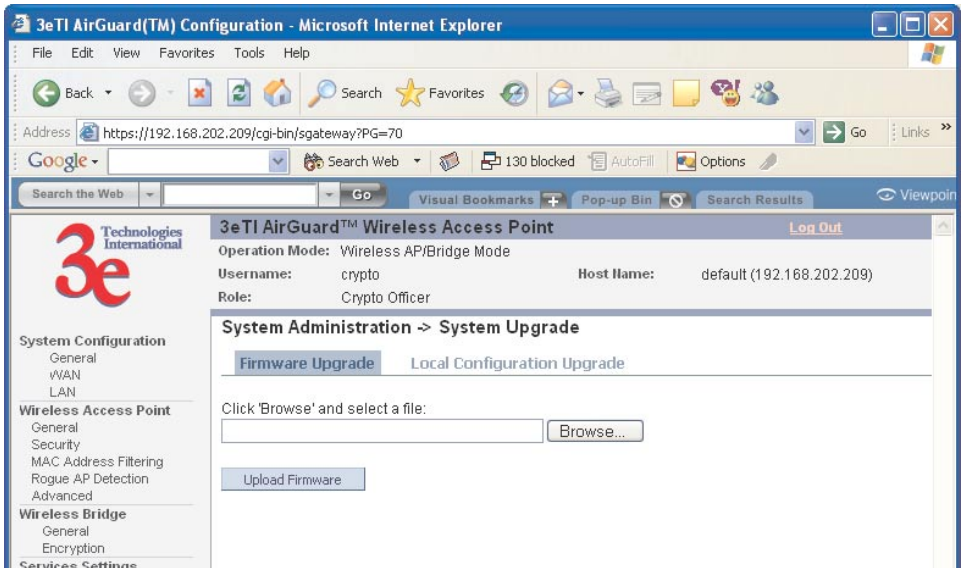
There is also a configuration file transfer option which allows the system configuration file from one AP to be transferred to another AP, in order to minimize the administration of the APs. Only configuration parameters that can be shared between APs are downloaded in the configuration file. WAN IP address and hostname are not transferred in the configuration file. Click on the **Local Configuration Upgrade** tab to perform file transfers.

Only the Crypto Officer role can access this function.

Firmware Upgrade

On the **System Administration — System Upgrade** screen, the Firmware Upgrade tab is the default view.

Click browse and select the firmware file to be uploaded. Click on the Upload Firmware button.

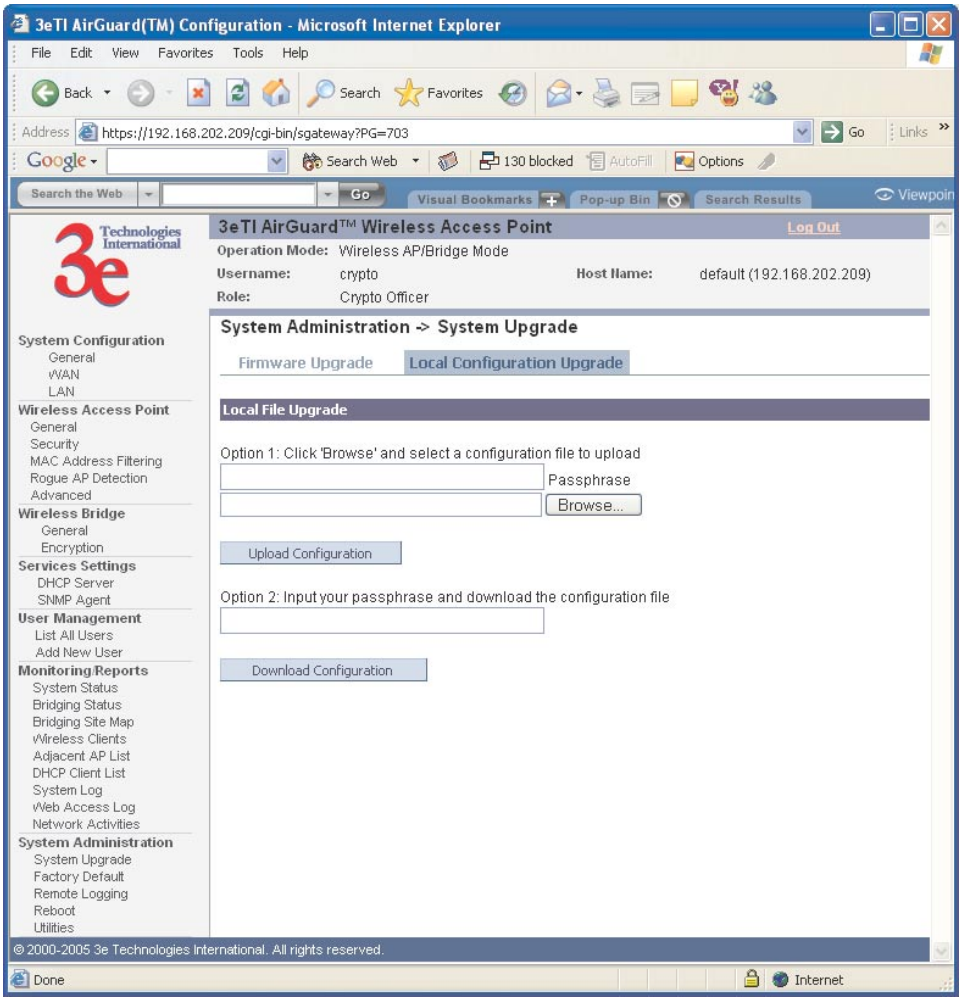


Local Configuration Upgrade

On the **System Administration — System Upgrade** screen, click on the **Local Configuration Upgrade** tab to upload and download configuration files to access points connected to the network.

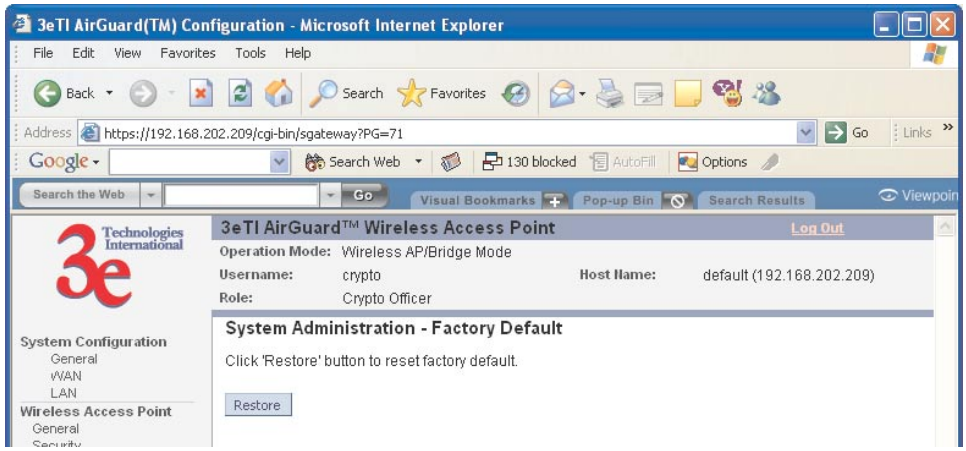
To upload a configuration file, select the file using the browse button and enter the passphrase for that file. The passphrase protects the file from unauthorized users. It prevents unauthorized users from applying the system configuration file to an unauthorized AP to gain access to the network. Before downloading the system configuration file to a local computer, the user must enter a passphrase to protect the file. Before the system configuration file can be uploaded onto another AP, the passphrase must be entered on the remote AP.

The configuration file can be tagged with a 12 character tag to keep track of the configuration file as it is transferred to other APs.



Factory Default

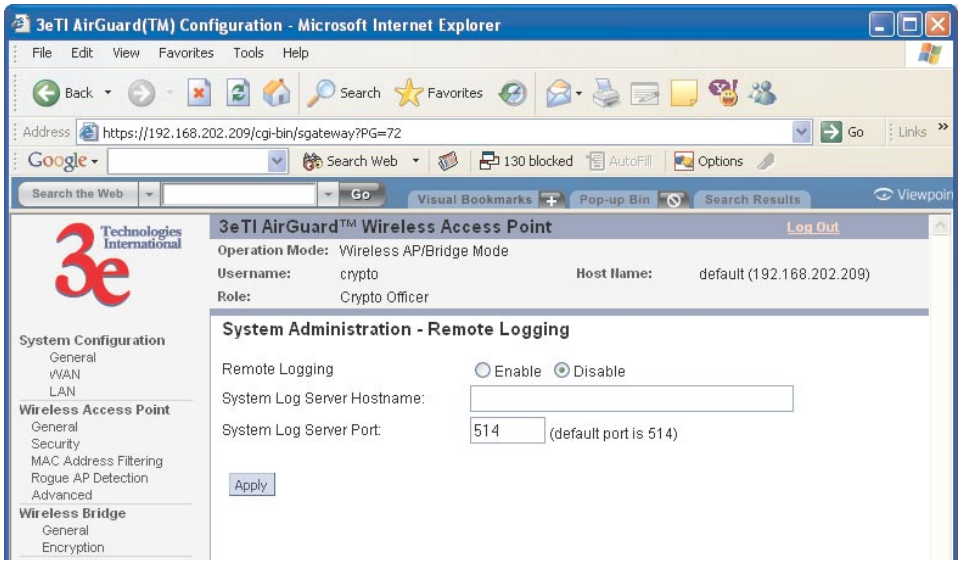
The **System Administration — Factory Default** screen is used to reset the AP to its factory settings. The "**Restore**" button is a fallback trouble-shooting function that should only be used to reset to original settings. Only the Crypto Officer role has access to the **Restore** button.



You can also reset the 3e–525C–2 to its factory default by pressing and holding the reset button located on the front of the unit for 10 seconds. Input is acknowledged by the WLANNSS LED turning on and then turning off after 10 seconds.

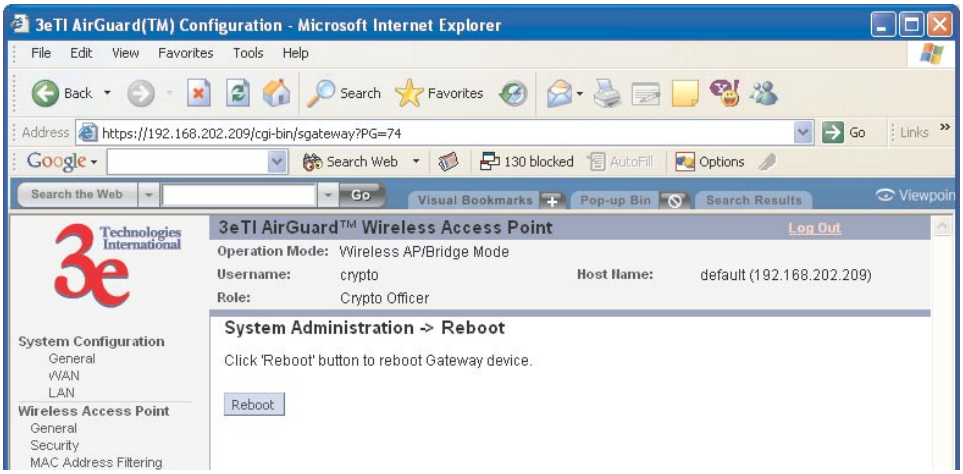
Remote Logging

The **System Administration —Remote Logging** screen allows you to forward the syslog data from each machine to a central remote logging server. In the 3e–525C–2, this function uses the **syslogd** daemon. If you enable Remote Logging, input a System Log Server IP Address and System Log Server Port. Click **Apply** to accept these values.



Reboot

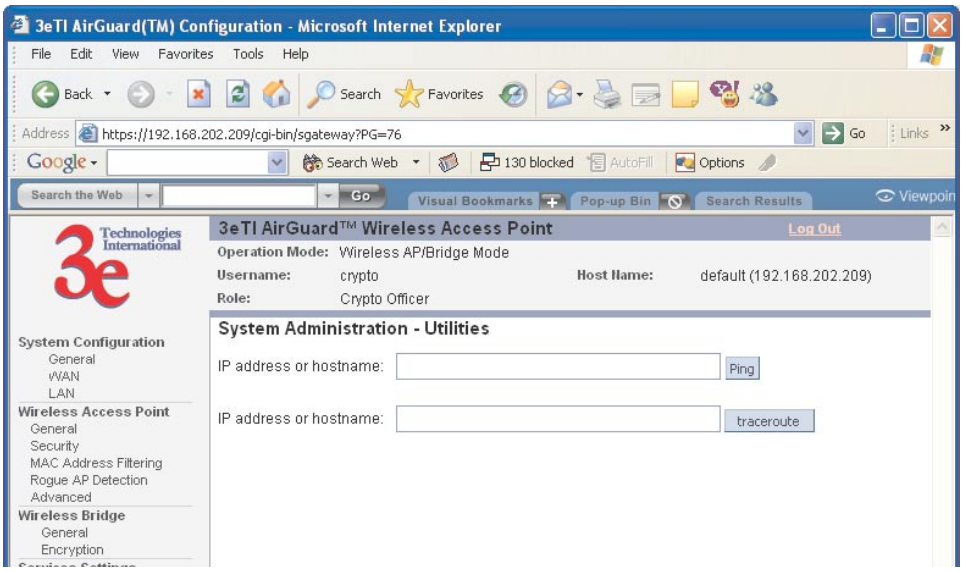
The **System Administration — Reboot** screen allows you to reboot the 3e–525C–2 without changing any preset functionality. Both Crypto Officer and Administrator functions have access to this function.



You can also reboot the 3e–525C–2 by pressing and holding the reset button on the front of the unit for five seconds. Input is acknowledged by the LWLANSS LED turning on.

Utilities

The **System Administration — Utilities** screen gives you ready access to two useful utilities: Ping and Traceroute. Simply enter the IP Address or hostname you wish to ping or traceroute and click either the **Ping** or **Traceroute** button, as appropriate.



Chapter 4: Wireless Bridge Configuration

Introduction

In the 3e–525C–2, wireless bridging uses a second WLAN card to set up an independent wireless bridge connection. Since wireless bridging provides a mechanism for APs to collaborate, it is possible to extend the basic service set (BSS) of a standalone AP and to connect two separate LANs without installing any cabling.

The wireless bridging function in the 3e–525C–2 supports a number of bridging configurations. Some of the most popular settings are discussed in this chapter:

- **Point-to-point bridging of two Ethernet links**
- **Point-to-multipoint bridging of several Ethernet links**
- **Repeater mode**

The wireless bridging screens are the same whether you are in access point or gateway mode.

Bridging is a function that is set up in addition to basic access point setup. If you will be using the 3e–525C–2 solely as a bridge, some of the settings you may have selected for access point use will not be necessary.

If setting up as a bridge during initial setup, you can either use the LAN Port directly wired by Ethernet cable to a laptop to set the appropriate settings. The management screens that you may need to modify, regardless of what type of bridging mode you choose, will be in the **Wireless Bridge** section of the navigation bar. These include:

- **Wireless Bridge — Bridging**
- **Wireless Bridge — Encryption**

NOTE: When the 3e–525C–2 is used as an access point, it is recommended that you do not use 802.11g Super mode for the bridge. The 802.11g Super mode uses large frequency bandwith and it may interfere with other AP radio signals.

Wireless Bridge — General

The **Wireless Bridge — General** screen contains wireless bridging information including the channel number, Tx rate, Tx power, spanning tree protocol (802.1d) enable/disable, and remote AP's BSSID. This page is important in setting up your bridge configuration. Wireless bridging supports two modes of operation:

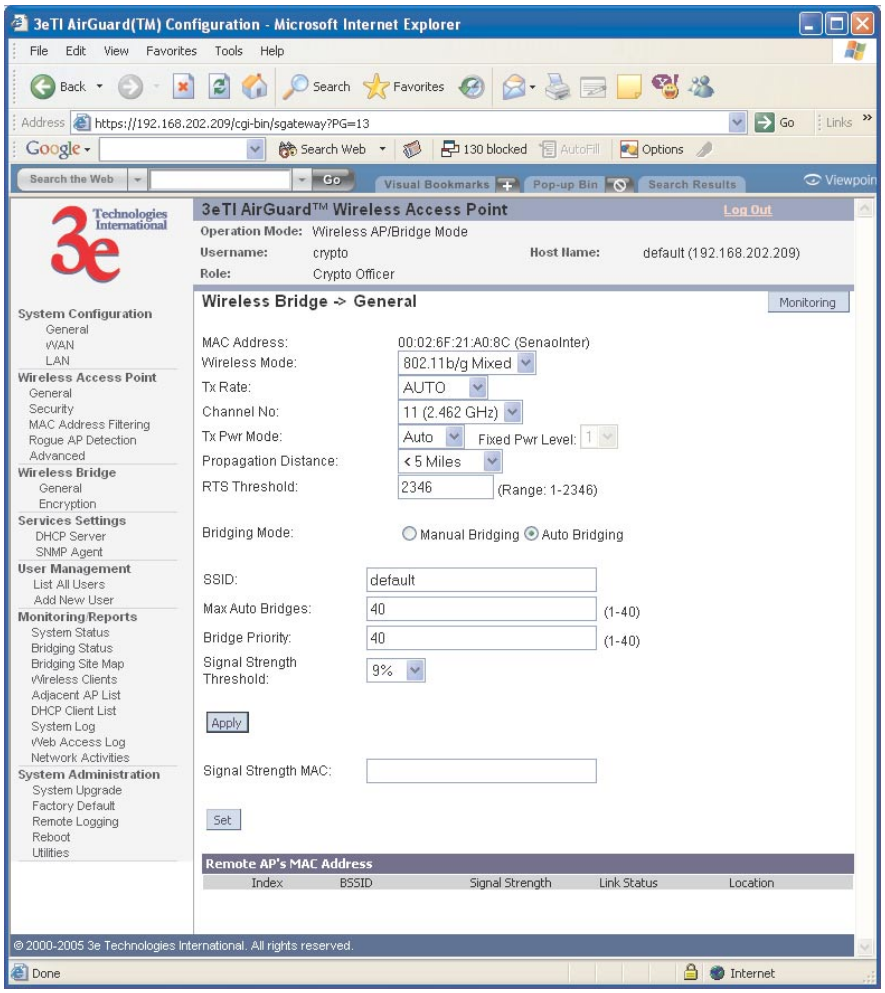
- Manual wireless bridging
- Auto-forming wireless bridging (AWB) - with a maximum number of allowable bridges (the default is 40)

Auto-forming Wireless Bridging

When the wireless bridge is in auto-forming mode, the wireless bridge sniffs for beacons from other wireless bridges and identifies APs that match a policy such as SSID and channel.

Instead of simply adding the APs with the same SSID/channel to the network, a three-way association handshake is performed in order to control network access.

To make a unit the root (leaf) STP node, set the bridge priority lower than any other node in the network.

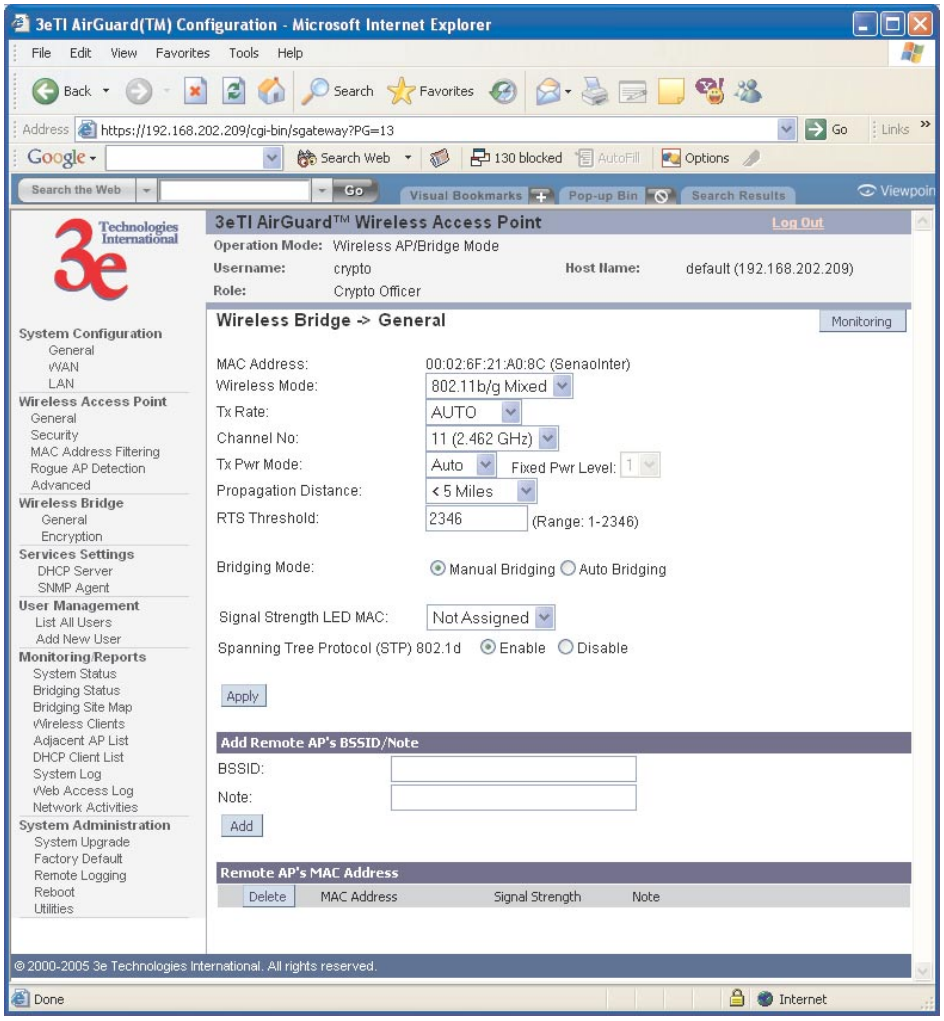


AUTO BRIDGING GENERAL SETTINGS OPTIONS		
Wireless Mode	802.11b/g Mixed 802.11g Super 802.11a 802.11a Turbo	Sets the wireless mode for the wireless bridge.
Tx Rate	**802.11b/g Mixed**	
	AUTO, 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54 Mbps	When set to AUTO, the card attempts to select the optimal rate for the channel. If a fixed rate is used, the card will only transmit at that rate.
	802.11g Super	
	AUTO	The card attempts to select the optimal rate for the channel.
	802.11a	
	AUTO, 6, 9, 12, 18, 24, 36, 48, 54 Mbps	When set to AUTO, the card attempts to select the optimal rate for the channel. If a fixed rate is used, the card will only transmit at that rate.
	802.11a Turbo	
	AUTO	The card attempts to select the optimal rate for the channel.
Channel No.	**802.11b/g Mixed**	
	1 (2.412 GHz) 2 (2.417 GHz) 3 (2.422 GHz) 4 (2.427 GHz) 5 (2.432 GHz) 6 (2.437 GHz) 7 (2.442 GHz) 8 (2.447 GHz) 9 (2.452 GHz) 10 (2.457 GHz) 11 (2.462 GHz)	Sets the channel frequency for the wireless bridge.
	802.11g Super	
	6 (2.437 GHz)	Sets the channel frequency for the wireless bridge.
	802.11a	
	52 (5.26 GHz) 56 (5.28 GHz) 60 (5.30 GHz) 64 (5.32 GHz) 149 (5.745 GHz) 153 (5.765 GHz) 157 (5.785 GHz) 161 (5.805 GHz) 165 (5.825 GHz)	Sets the channel frequency for the wireless bridge.
	802.11a Turbo	
	50 (5.25 GHz) Turbo Mode 58 (5.29 GHz) Turbo Mode 152 (5.76 GHz) Turbo Mode 160 (5.80 GHz) Turbo Mode	Sets the channel frequency for the wireless bridge.

Tx Pwr Mode	OFF FIXED, AUTO	The Tx Pwr Mode defaults to AUTO, giving the largest range of radio transmission available under ambient conditions. The wireless bridge's broadcast range can be limited by setting the Tx Pwr Mode to Fixed and choosing from 1-5 for Fixed Pwr Level. If you want to prevent any radio frequency transmission from the wireless bridge, set the Tx Pwr Mode to OFF. This will not turn off RF transmissions from any associated wireless devices, but they will not be able to communicate with the wireless bridge when the Tx Pwr Mode is off.
Fixed Pwr Level	1, 2, 3, 4, 5	Select a range when Rx Pwr Mode is set to FIXED. Level 1 is the shortest distance (Level 1=7dBm) and Level 5 is the longest (Level 5=15dBm)
Propagation Distance	< 5 Miles 5-10 Miles 11-15 Miles 16-20 Miles 21-25 Miles 26-30 Miles > 30 Miles	Set the distance based on the distance between this bridge and furthest bridge that is connected to it.
Bridging Mode	Auto Bridging	auto bridging selected
SSID		Can be any set of letters and numbers assigned by the network administrator. This nomenclature has to be set on the wireless bridge and each wireless device in order for them to communicate.
Max Auto Bridges	1-40	Maximum number of auto bridges allowed.
Bridge Priority	1-40	Determines the root (leaf) STP node. The lowest bridge priority in the network will become the STP root.
Signal Strength MAC		The signal strength of this wireless bridge will be indicated on the Signal Strength LED located on the front of the case.

Manual Bridging

When the wireless bridge is in manual bridging mode, you can manually add the MAC address of the remote bridge.

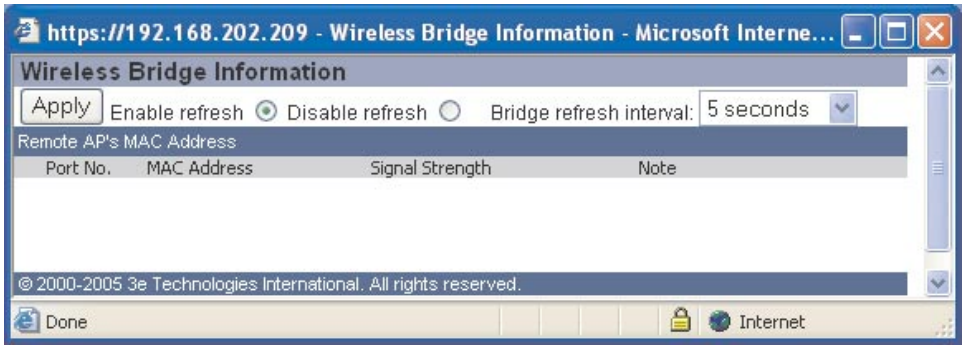


MANUAL BRIDGING GENERAL SETTINGS OPTIONS		
Wireless Mode	802.11b/g Mixed 802.11g Super 802.11a 802.11a Turbo	Sets the wireless mode for the wireless bridge.
Tx Rate	**802.11b/g Mixed**	
	AUTO, 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54 Mbps	When set to AUTO, the card attempts to select the optimal rate for the channel. If a fixed rate is used, the card will only transmit at that rate.
	802.11g Super	
	AUTO	The card attempts to select the optimal rate for the channel.
	802.11a	
	AUTO, 6, 9, 12, 18, 24, 36, 48, 54 Mbps	When set to AUTO, the card attempts to select the optimal rate for the channel. If a fixed rate is used, the card will only transmit at that rate.
	802.11a Turbo	
	AUTO	The card attempts to select the optimal rate for the channel.
Channel No.	**802.11b/g Mixed**	
	1 (2.412 GHz) 2 (2.417 GHz) 3 (2.422 GHz) 4 (2.427 GHz) 5 (2.432 GHz) 6 (2.437 GHz) 7 (2.442 GHz) 8 (2.447 GHz) 9 (2.452 GHz) 10 (2.457 GHz) 11 (2.462 GHz)	
	802.11g Super	
	6 (2.437 GHz)	
	802.11a	
	52 (5.26 GHz) 56 (5.28 GHz) 60 (5.30 GHz) 64 (5.32 GHz) 149 (5.745 GHz) 153 (5.765 GHz) 157 (5.785 GHz) 161 (5.805 GHz) 165 (5.825 GHz)	
	802.11a Turbo	
	50 (5.25 GHz) Turbo Mode 58 (5.29 GHz) Turbo Mode 152 (5.76 GHz) Turbo Mode 160 (5.80 GHz) Turbo Mode	

Tx Pwr Mode	OFF FIXED, AUTO	The Tx Pwr Mode defaults to AUTO, giving the largest range of radio transmission available under ambient conditions. The wireless bridge's broadcast range can be limited by setting the Tx Pwr Mode to Fixed and choosing from 1-5 for Fixed Pwr Level. If you want to prevent any radio frequency transmission from the wireless bridge, set the Tx Pwr Mode to OFF. This will not turn off RF transmissions from any associated wireless devices, but they will not be able to communicate with the wireless bridge when the Tx Pwr Mode is off.
Fixed Pwr Level	1, 2, 3, 4, 5	Select a range when Rx Pwr Mode is set to FIXED. Level 1 is the shortest distance (Level 1=7dBm) and Level 5 is the longest (Level 5=15dBm)
Propagation Distance	< 5 Miles 5-10 Miles 11-15 Miles 16-20 Miles 21-25 Miles 26-30 Miles > 30 Miles	Set the distance based on the distance between this bridge and furthest bridge that is connected to it.
Bridging Mode	Manual Bridging	manual bridging selected
Signal Strength LED MAC		Allows you to set the number of one of the Remote APs which will be listed at the bottom of the screen once the system is operational This wireless bridge becomes the guiding port that is displayed in the WLANNSS LED on the front of the 3e–525C–2 as a signal.
Spanning Tree Protocol (STP)	Enable/Disable	Enable STP is there is any possiblity that a bridging loop could occur. If you are certain that there is no possibility that a bridging loop will occur, then disalbe STP. The bridge will be more efficient (faster) without it. If you are not sure, the safest solution is to enable STP.
BSSID	Enter hexadecimal numbers	Add the MAC address of the remote bridge. The remote bridge's MAC address will appear at the bottom of the screen.
Note		You can enter a note that defines the location of the remote bridge.

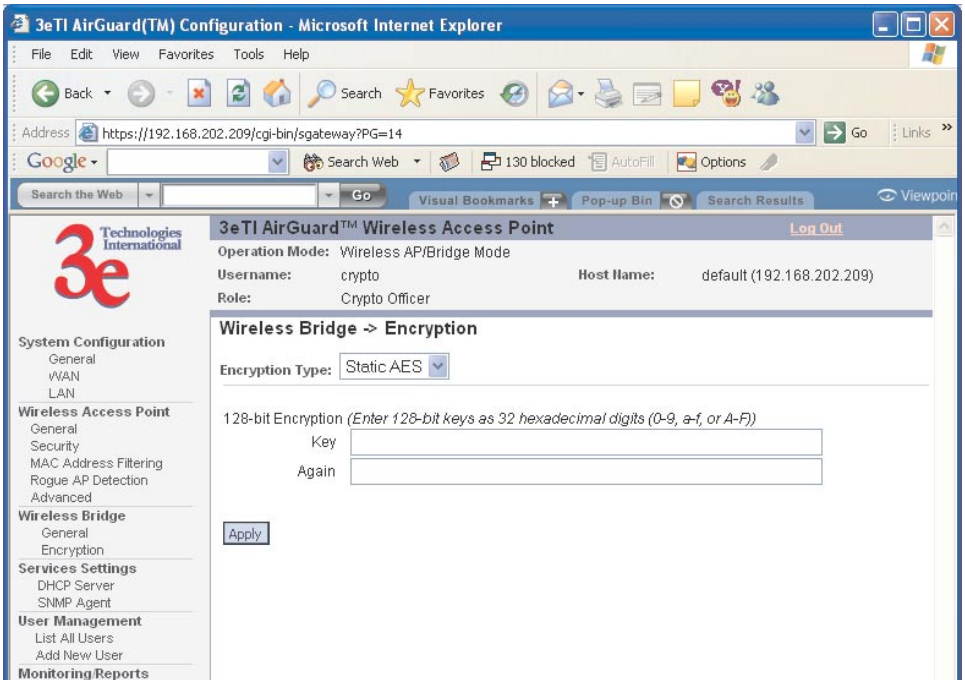
Monitoring

In the upper right-hand corner of the **Wireless Bridge — General** screen there is a button called Monitoring. f you click on this button, a pop-up window will appear (WDS Information). If you select Enable refesh, you can set the bridge refresh interval from 5 seconds to 30 minutes. Refreshing the screen allows you to see the effect of aiming the antenna to improve signal strength.



Wireless Bridge — Encryption

The **Wireless Bridge — Encryption** screen is used to configure static encryption keys for the wireless bridge. This is an important page to set up to ensure that your bridge is working correctly. The encryption key that you use on this screen must be the same for any bridge connected to your bridging network in order for communication to occur. On this screen you can select None or Static AES (128-bit).

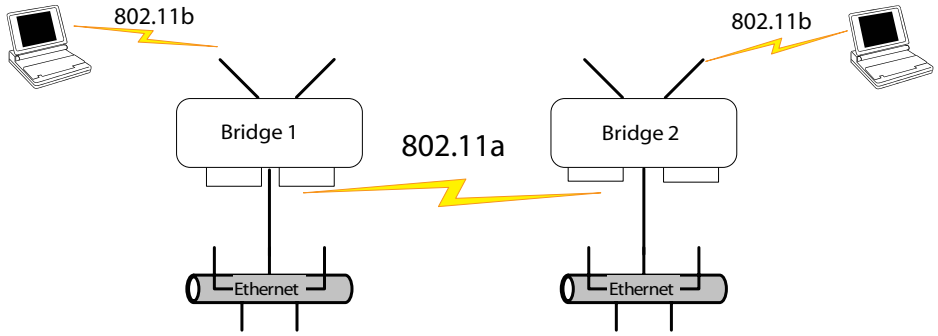


The following sections describe the setup for three types of bridging configuration: point-to-point, point-to-multipoint, or, lastly, repeater.

Setting Up Bridging Type

Point-to-Point Bridge Configuration

A point-to-point link is a direct connection between two, and only two, locations or nodes. Because the bridge function uses a separate WLAN card for bridging, you can also set up WLANs on the separate AP WLAN card.



For the two bridges that are to be linked to communicate properly, they must be set up with compatible commands in the setup screens.

For instance, the bridges must have the same channel number. Because there is a separate WLAN card for bridging, there can be a separate WLAN on the AP WLAN card with no loss efficiency, as long as you set the channel numbers so there's no conflict or noise with the channel assigned to the bridge. Spanning Tree Protocol may be set to Enable, if there is any possibility of a bridging loop, or to Disable (which is more efficient) if there's no possibility of a bridging loop. Each bridge must contain the other's BSSID. (The BSSID of each is equivalent to the MAC address contained on the **Wireless Bridge — General** setup page. Enter only hexadecimal numbers, no colons. Data entry is not case sensitive.) Finally, the wireless bridging encryption must be set to the appropriate type and key length and must be identical on each bridge.

The following charts show sample settings for manual bridging and auto bridging modes.

Point-to-Point Bridging Setup Guide - Manual Mode

Direction	Bridge 1	Bridge 2
Wireless Bridge — General (Manual Bridging Mode)		
Wirelss Mode	802.11a	802.11a
Tx Rate	AUTO	AUTO
Channel No.	Must be the same as Bridge 2	Must be the same as Bridge 1
Tx Power	Auto	Auto
Propagation Distance	< 5 Miles	< 5 Miles
Bridging Mode	manual briding selected	manual bridging selected
Signal Strength LED MAC	Not Assigned (select from drop-down list)	Not Assigned (select from drop-down list)
Spanning Tree Protocol (STP)	Enable (or Disable if no bridging loop possible)	Enable (or Disable if no bridging loop possible)
BSSID	Add Bridge 2 MAC	Add Bridge 1 MAC
Wireless Bridge — Encryption		
Bridging encryption options	Select appropriate key type/length and value. Must be the same key as Bridge 2.	Select appropriate key type/length and value. Must be the same key as Bridge 1.

Point-to-Point Bridging Setup Guide - Auto Mode

Direction	Bridge 1	Bridge 2
Wireless Bridge — Genral (Auto Bridging Mode)		
Wirelss Mode	802.11a	802.11a
Tx Rate	AUTO	AUTO
Channel No.	Must be the same as Bridge 2	Must be the same as Bridge 1
Tx Power Mode	Auto	Auto
Propagation Distance	< 5 Miles	< 5 Miles
Bridging Mode	Auto bridging selected	Auto bridging selected
SSID	Must be the same as Bridge 2	Must be the same as Bridge 1
Max Auto Bridges	40 (range 1-40)	40 (range 1-40)
Bridge Priority	40 (range 1-40)	40 (range 1-40)
Signal Strength MAC	Enter from list at the bottom of the screen	Enter from list at the bottom of the screen
Wireless Bridge — Encryption		
Bridging encryption options	Select appropriate key type/length and value. Must be same as Bridge 2.	Select appropriate key type/length and value. Must be same as Bridge 1.
Wireless Bridge — MAC Address Filtering		
MAC Address Filtering options	Select Filter Type: input MAC addresses	Select Filter Type: input MAC addresses

The following sequence walks you through the setup of bridge 1. Bridge 2 would duplicate this procedure, with the BSSID of bridge 2 being the MAC address of bridge 1 and vice versa.

Navigate to the **Wireless Bridge — General** screen.

In the first section: **General**, you will see the MAC Address of the bridging card. This is used as the BSSID on other 3e–525C–2s that will be communicatingwith this one.

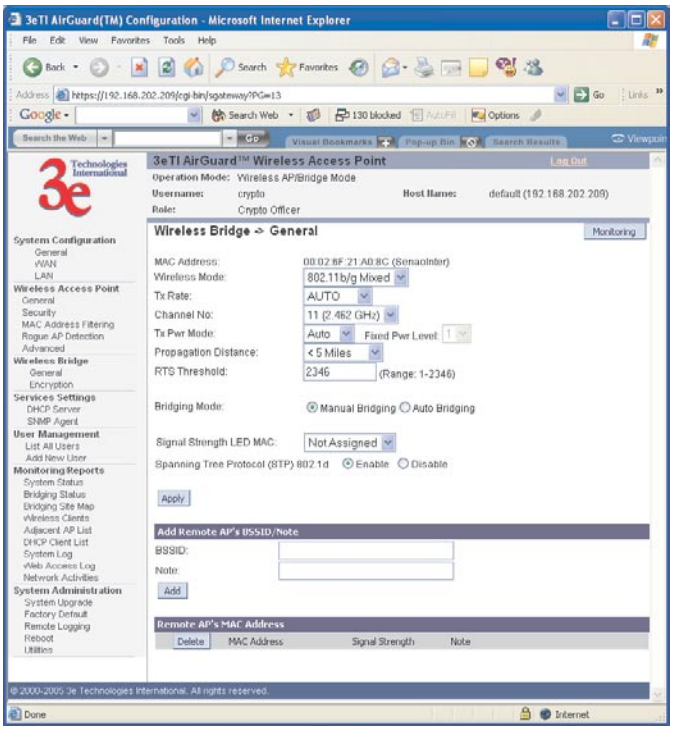
Wireless Mode is set to 802.11a. Set Basic and Supported Rates. **Channel Number** must be set the same for each bridge to communicate. **TX Pwr Mode** can be left on **Auto** unless the power needs to be regulated. Set **Spanning Tree Protocol** to **Enable** unless you are sure that there is no chance of a loop.

Click **Apply** to accept your changes but remain on this screen.

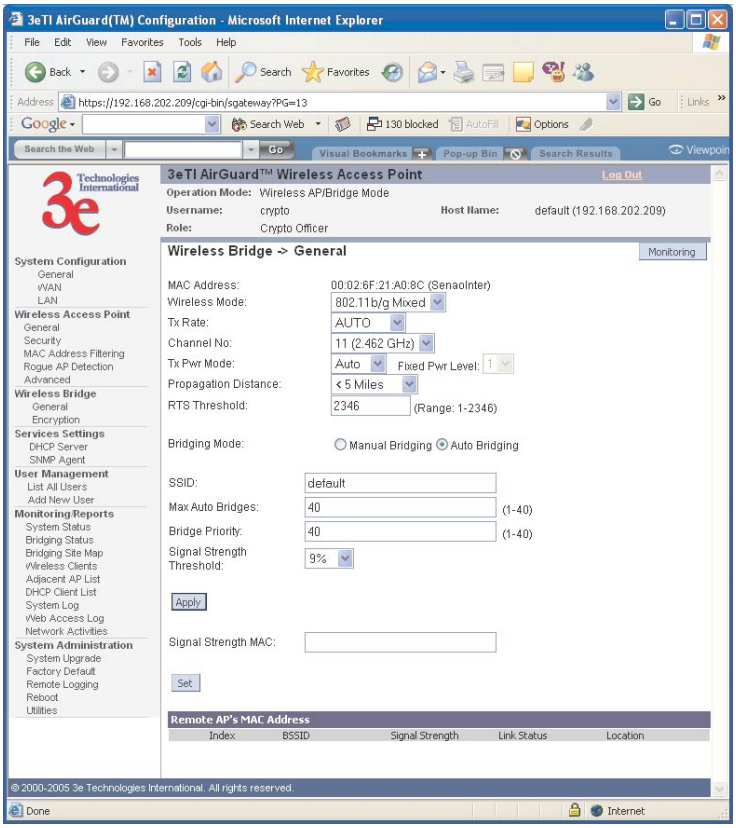
Next is **Bridging Mode**. Select either manual or auto bridging. If you choose manual then you will have to manually add the BSSID of the remote bridge. The BSSID corresponds to that bridge's MAC address. In entering the BSSID, enter only hexadecimal numbers, no colons. Data entry is not case sensitive. You may also enter a note that defines the location of the remote bridge. Then click **Add** to accept. The remote bridge's BSSID will now appear at the bottom of the page. If, at some time you wish to delete the entry, simply click the check box next to it and confirm by clicking **Delete**.

Signal strength LED MAC allows you to set the number of one of the Remote APs which will be listed at the bottom of the screen once the system is operational as the guiding port that you wish to have display in the WLANSS LED on the front of the 3e–525C–2 as a signal. If you don't wish to display any connection signal, simply leave this set at Not Assigned.

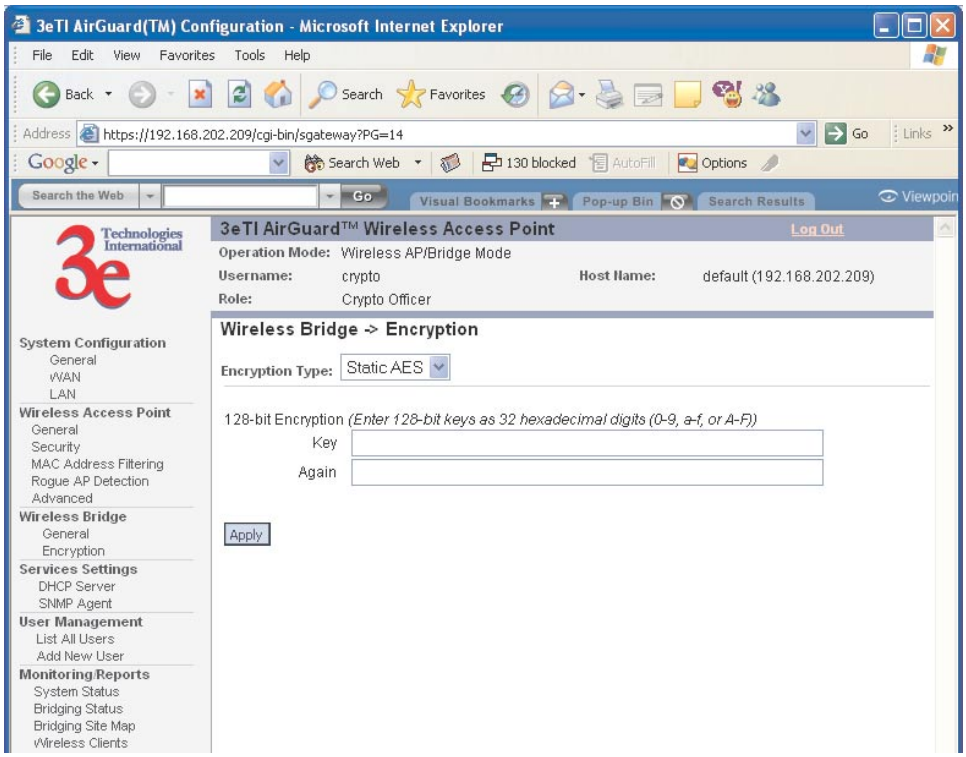
Then click **Apply** to accept.



If you choose auto bridging mode, then enter the **Max Auto Bridges** (range from 1-40), **Bridge Priority** (range from 1-40), and the **Signal Strength MAC**.



Next, navigate to the **Wireless Bridge — Encryption** screen. Select the appropriate key type and length and the key value. The encryption key value and type for Bridge 1 must be the same as for Bridge 2. For wireless bridging, only AES is available for encryption.



You must complete the configuration of your Bridge 1 by following the general instructions in Chapter 3 of this guide to establish any other required configuration options such as General, WAN and LAN settings.

Configure the second of your two point-to-point bridges following the instructions given for Bridge 1 above.

Point-to-Multipoint Bridge Configuration

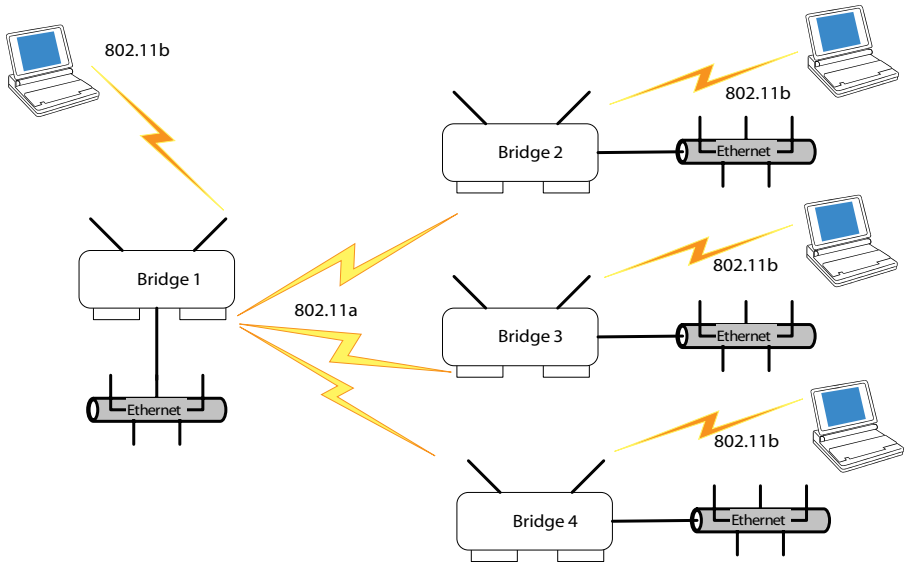
A point-to-multipoint configuration allows you to set up three or more 3e–525C–2 access points in bridging mode and accomplish bridging between 3 or more locations wirelessly.

For the three bridges that are to be linked to communicate properly, they have to be set up with compatible commands in their setup screens.

For instance, all bridges must have the same channel number. Spanning Tree Protocol will usually be set to Enable. If configured as in the diagram following, Bridge 1 must contain all of the others' BSSIDs, while Bridge 2 ~ n must only contain Bridge 1's BSSID. (The BSSID of each is equivalent to the MAC address found on the **Wireless Bridge — General** page. Enter only hexadecimal numbers. Data entry is not case sensitive.) Finally, the wireless bridging encryption of each must be set to the appropriate type and key length and must be the same on all.

Because the 3e–525C–2 has two separate WLAN cards, one for the AP and one for the Bridge, each bridge can have a WLAN on the 802.11a protocol with no loss of efficiency in bridging if you wish.

The following diagram pictures a point-to-multipoint setup, which might be of use where a company's network spans several buildings within a campus-like setting.



Follow the steps of the procedure outlined in the point-to-point bridge section. The chart following describes the basic attributes.

Point-to-Multipoint Bridging Setup Guide - Manual Mode

Direction	Bridge 1	Bridge 2 ~ n
Wireless Bridge — General (Manual Bridging Mode)		
Wirelss Mode	802.11a	802.11a
Tx Rate	AUTO	AUTO
Channel No.	Same as Bridge 2~n	Same as Bridge 1
Tx Power	Auto	Auto
Propagation Distance	< 5 Miles	< 5 Miles
Bridging Mode	manual bridging selected	manual bridging selected
Signal Strength LED MAC	Not Assigned (select from drop-down list)	Not Assigned (select from drop-down list)
Spanning Tree Protocol	Enable (or Disable if no bridging loop possible)	Enable (or Disable if no bridging loop possible)
BSSID	Add Bridge 2~n MAC	Add Bridge 1 MAC
Wireless Bridge — Encryption		
Bridging encryption options	Select appropriate key type/length and value. Must be the same key as Bridge 2~n.	Select appropriate key type/length and value. Must be the same key as Bridge 1.

Point-to-Multipoint Bridging Setup Guide - Auto Mode

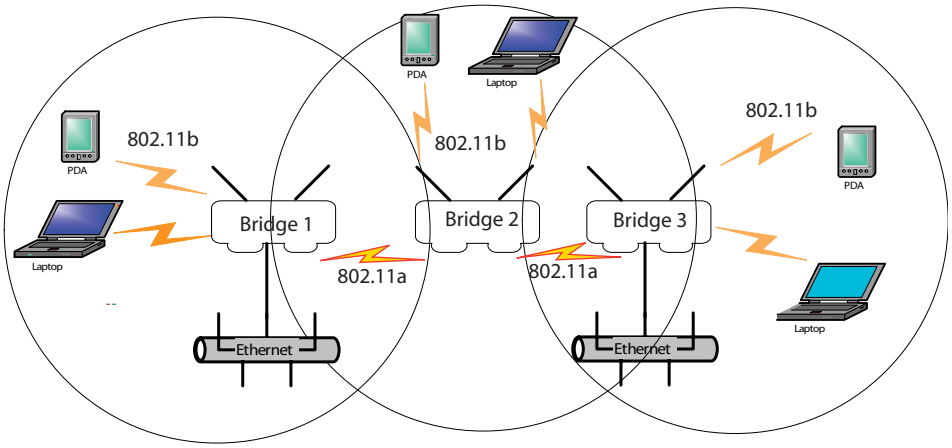
Direction	Bridge 1	Bridge 2 ~ n
Wireless Bridge — General (Auto Bridging Mode)		
Wirelss Mode	802.11a	802.11a
Tx Rate	AUTO	AUTO
Channel No.	Same as Bridge 2~n	Same as Bridge 2~n
Tx Power Mode	Auto	Auto
Propagation Distance	< 5 Miles	< 5 Miles
Bridging Mode	Auto bridging selected	Auto bridging selected
SSID	Must be the same as Bridge 2~n	Must be the same as Bridge 2
Max Auto Bridges	40 (range 1-40)	40 (range 1-40)
Bridge Priority	40 (range 1-40)	40 (range 1-40)
Signal Strength MAC	Enter from list at the bottom of the screen	Enter from list at the bottom of the screen
Wireless Bridge — Encryption		
Bridging encryption options	Select appropriate key type/length and value. Must be same as Bridge 2.	Select appropriate key type/length and value. Must be same as Bridge 2.
Wireless Bridge — MAC Address Filtering		
MAC Address Filtering options	Select Filter Type: input MAC addresses	Select Filter Type: input MAC addresses

The above recommended setup requires only Bridge 1 to be set in point-to-multipoint mode. It is possible to set all bridges in point-to-multipoint mode, in which case , each bridge would have to contain the BSSID for each of the other bridges and Spanning Tree Protocol must be Enabled.

As stated previously, complete any other setup screens following general instructions in Chapter 3.

Repeater Bridge Configuration

A repeater setup can be used to extend the wireless signal from one bridge connected to an Ethernet LAN wirelessly so that another bridge can control a wireless LAN at a distance.



Repeater Bridging Setup Guide - Manual Mode

Direction	Bridge 1	Bridge 2	Bridge 3
Wireless Bridge — General (Manual BridgingMode)			
Wireless Mode	802.11a	802.11a	802.11a
Tx Rate	AUTO	AUTO	AUTO
Channel	Same as Bridge 2	Same as Bridge 1	Same as Bridge 1
Tx Power Mode	Auto	Auto	Auto
Propagation Distance	< 5 Miles	< 5 Miles	< 5 Miles
Bridging Mode	manual	manual	manual
Signal Strength LED MAC	Not Assigned (select from drop-down list)	Not Assigned (select from drop-down list)	Not Assigned (select from drop-down list)
Spanning Tree Protocol	Enable (or Disable if no bridging loop possible)	Enable (or Disable if no bridging loop possible)	Enable (or Disable if no bridging loop possible)
BSSID	Add Bridge 2's MAC	Add Bridge 1's and Bridge 3's MAC	Add Bridge 2's MAC
Wireless Bridge — Encyption			
Wireless Configuration – Bridging Encryption	Select appropriate key type/length and enter key value. Must be the same as that on the other 2 Bridges.	Select appropriate key type/length and enter key value. Must be the same as that on the other 2 Bridges.	Select appropriate key type/length and enter key value. Must be the same as that on the other 2 Bridges.

Repeater Bridging Setup Guide - Auto Mode

Direction	Bridge 1	Bridge 2	Bridge 3
Wireless Bridge — General (Auto Bridging Mode)			
Wireless Mode	802.11a	802.11a	802.11a
Tx Rate	AUTO	AUTO	AUTO
Channel	Same as Bridge 2	Same as Bridge 1	Same as Bridge 1
Tx Power Mode	Auto	Auto	Auto
Propagation Distance	< 5 Miles	< 5 Miles	< 5 Miles
Bridging Mode	auto	auto	auto
SSID	Must be the same as Bridge 2	Must be the same as Bridge 1	Must be the same as Bridge 1
Max Auto Bridges	40 (range 1-40)	40 (range 1-40)	40 (range 1-40)
Bridge Priority	40 (1-40)	40 (1-40)	40 (1-40)
Signal Strength MAC	Enter from list at the bottom of the screen	Enter from list at the bottom of the screen	Enter from list at the bottom of the screen
Wireless Bridge — Encyption			
Wireless Configuration – Bridging Encryption	Select appropriate key type/length and enter key value. Must be the same as that on the other 2 Bridges.	Select appropriate key type/length and enter key value. Must be the same as that on the other 2 Bridges.	Select appropriate key type/length and enter key value. Must be the same as that on the other 2 Bridges.
Wireless Bridge — MAC Address Filtering			
MAC Aaddress Filtering options	Select Filter Type: input MAC addresses	Select Filter Type: input MAC addresses	Select Filter Type: input MAC addresses

With this configuration, each bridge can control a wireless LAN. All wireless clients must have the same SSID as the bridges on the AP card channel. All clients can roam between the three bridges.

All other setup screens should be completed following the guidelines in Chapter 3.

Chapter 5: Technical Support

Manufacturer's Statement

The 3e–525C–2 is provided with warranty. It is not desired or expected that the user open the device. If malfunction is experienced and all external causes are eliminated, the user should return the unit to the manufacturer and replace it with a functioning unit.

If you are experiencing trouble with this unit, the point of contact is:

support@3eti.com

or visit our website at

www.3eti.com

Radio Frequency Interference Requirements

This device has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission's Rules and Regulations. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Installation should be accomplished using the authorized cables and/or connectors provided with the device or available from the manufacturer/distributor for use with this device. Changes or modifications not expressly approved by the manufacturer or party responsible for this FCC compliance could void the user's authority to operate the equipment.

This page intentionally left blank.

Glossary

802.11

802.11 refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997.

802.11b (also referred to as 802.11 High Rate or WiFi)

802.11b is an extension to 802.11 that applies to wireless LANs and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.

Access Point

An access point is a gateway set up to allow a group of LAN users access to another group or a main group. The access point doesn't use the DHCP server function and therefore accepts IP address assignment from the controlling network.

AES

Short for Advanced Encryption Standard, a symmetric 128-bit block data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously.

Bridge

A device that connects two local-area networks (LANs), or two segments of the same LAN that use the same protocol, such as Ethernet or Token-Ring.

DHCP

Short for Dynamic Host Configuration Protocol, DHCP is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address. Many ISPs use dynamic IP addressing for dial-up users.

NMS (Network Management Station)

Includes such management software as HP Openview and IBM Netview.

PC Card

A computer device packaged in a small card about the size of a credit card and conforming to the PCMCIA standard.

PDA (Personal Digital Assistant)

A handheld device.

SNMP

Simple Network Management Protocol

SSID

A Network ID unique to a network. Only clients and access points that share the same SSID are able to communicate with each other. This string is case-sensitive. Wireless LANs offer several security options, but increasing the security also means increasing the time spent managing the system. Encryption is the key. The biggest threat is from intruders coming into the LAN. You set a seven-digit alphanumeric security code, called an SSID, in each wireless device and they thereafter operate as a group.

TKIP

Temporal Key Integrity Protocol. TKIP is a protocol used in WPA. It scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

VPN (Virtual Private Network)

A VPN uses encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

WLAN (Wireless Local Area Network)

A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.

WPA

WPA stands for WiFi Protected Access. It's an interim standard developed by the WiFi Alliance pending full ratification of the 802.11i standard, to protect the wired band and improve upon the old WEP encryption standard.